Electronic Colloquium on Computational Complexity, Report No. 71 (2002)

Non-approximability of the Permanent of Structured Matrices over Finite Fields

Bruno Codenotti
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
Via Alfieri 1, Pisa, 56010–Ghezzano, Italy
codenotti@imc.pi.cnr.it

and

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

September 11, 2002

Abstract

We show that for several natural classes of "structured" matrices, including symmetric, circulant, Hankel and Toeplitz matrices, approximating the permanent modulo a prime p is as hard as computing the exact value. Results of this kind are well known for the class of arbitrary matrices; however the techniques used do not seem to apply to "structured" matrices. Our approach is based on recent advances in the hidden number problem introduced by Boneh and Venkatesan in 1996 combined with some bounds of exponential sums.

ISSN 1433-8092

1 Introduction

Let $\mathbb{F}_p$ denote a finite field of p elements.

Given a matrix $X = (x_{ij})_{i,j=1}^n$ over $\mathbb{F}_p$, we denote by $\operatorname{per} X$ its *permanent*.

It is well know that the permanent is very hard to evaluate exactly. In technical terms, the permanent is $\sharp\mathbf{P}$-complete. Thus in a number of papers various *approximability* and *non-approximability* properties of the permanent have been considered, taking into account randomized algorithms as well. In particular, it has been shown by Cai et al. in [7] that randomized polynomial time algorithms cannot compute the permanent correctly even on a very small fraction of the instances, unless $\mathbf{P}^{\sharp\mathbf{P}} = \mathbf{BPP}$. Recall that the class $\sharp\mathbf{P}$ is the class of functions counting the number of accepting computations in a nondeterministic polynomial time Turing machine (see [24]), while the class $\mathbf{BPP}$ is the equivalent of the class $\mathbf{P}$ for probabilistic computations (with bounded error).

Note that the above mentioned "non-approximability" results as well as the results of many other works, see [7, 11, 14, 17] and references therein, apply to arbitrary matrices. On the other hand, despite the a variety of results on computing peraments while for special classes of matrices very little seems to be known, see [2, 8, 9].

Here we propose an alternative approach which allows us to obtain "non-approximability" results for matrices with some special structure, for example, symmetric, circulant, Hankel, and Toeplitz matrices. For all these classes of matrices over $\mathbb{F}_p$ we prove that if computing the permanent is *hard* then approximating the permanent is *hard* as well.

This approach certainly applies to general matrices as well, although in this case Theorems 1.7 and 1.9 of [11] give a much stronger result. However the method of proof does not apply to structured matrices. Indeed, the transformation described in the proof of Theorem 5.2 of [11] does not preserve structural properties as being symmetric or Toeplitz.

Our method takes advantage of recent advances in the *hidden number problem*, a problem introduced by Boneh and Venkatesan [3, 4]. The approach of [3, 4] (which is based on lattice reduction algorithms) combined with exponential sum techniques has led to a number of results in cryptography and complexity theory [10, 12, 13, 16, 18, 19, 21, 22, 23].

Here we show that the above combination of two celebrated techniques, lattice reduction and bounds of exponential sums, can be applied to studying the permanent.

For integers s and $m \geq 1$ we denote by $\lfloor s \rfloor_m$ the remainder of s on division by m.

For an integer m and a real $k > 0$ we denote by $\mathrm{APPROX}_{k,m}(t)$ any integer u which satisfies the inequality

$$|\lfloor t \rfloor_m - u| < \frac{m}{2^k}. \tag{1}$$

Thus, roughly speaking, $\mathrm{APPROX}_{k,m}(t)$ is the integer defined by the k most significant bits of $\lfloor t \rfloor_m$. However, this definition is more flexible and better suited to our purposes. In particular we remark that k in inequality (1) needs not be an integer.

We always assume that the field $\mathbb{F}_p$ consists of elements $\{0, \ldots, m-1\}$, so that we can apply $\mathrm{APPROX}_{k,p}$ to elements of $\mathbb{F}_p$.

Using the above notation, we can formulate the hidden number problem as follows: Let $\alpha \in \mathbb{F}_p$. Assuming we have access to values $\mathrm{APPROX}_{k,p}(\alpha t)$, for some $k > 0$, and for many known random values $t \in \mathbb{F}_p^*$, recover the number α.

It is clear that the only case of interest occurs when $k < \log p$; in [3] a polynomial time algorithm has been given which recovers α for $k \sim \log^{1/2} p$. However it has turned out that for many applications the property that t is randomly selected from $\mathbb{F}_p$ is too restrictive, see [10, 12, 13, 16, 18, 19, 21, 22, 23]. For those applications one has rather to study the case when t is selected at random from a certain sequence $\mathcal{T}$ of elements from $\mathbb{F}_p$. The above papers show that the uniformity of distribution properties of $\mathcal{T}$ play a crucial role, and thus exponential sums have been brought into the problem.

2 Auxiliary Results

We recall that the *discrepancy* $\mathcal{D}(\Omega)$ of a sequence $\Omega = \{\omega_1, \ldots, \omega_N\}$ of N elements of the interval $[0, 1]$ is defined as

$$\mathcal{D}(\Omega) = \sup_{J \subseteq [0,1]} \left| \frac{A(J, N)}{N} - |J| \right|,$$

where the supremum is extended over all subintervals J of $[0, 1]$, $|J|$ is the length of J, and $A(J, N)$ denotes the number of points ω_ν in J, for $0 \leq \nu \leq N - 1$. For our purposes we also need the following definition. We say that a finite sequence $\mathcal{T}$ of elements of $\mathcal{T}$ is Δ-*homogeneously distributed modulo*

p if for any $a \in \mathbb{F}_p^*$ the discrepancy of the sequence $\{\lfloor at \rfloor_p / p\}_{t \in \mathcal{T}}$ is at most Δ.

Lemma 1 *Let $\gamma > 0$ be an arbitrary absolute constant. For a prime p, define*

$$k = \left\lceil \gamma \left(\frac{\log p \log\log\log p}{\log\log p} \right)^{1/2} \right\rceil \qquad \text{and} \qquad d = \left\lceil \frac{3 \log p}{k} \right\rceil .$$

Let $\mathcal{T}$ be a 2^{-k}-homogeneously distributed modulo p sequence of integer numbers. There exists a probabilistic polynomial-time algorithm $\mathcal{A}$ such that for any $\alpha \in \mathbb{F}_p$, given as input the prime p, d integers $t_1, \ldots, t_d$, and d integers

$$u_i = \mathrm{APPROX}_{k,p}(\alpha t_i), \qquad i = 1, \ldots, d,$$

for sufficiently large p, its output satisfies

$$\Pr\left[\mathcal{A}\left(p, t_1, \ldots, t_d; u_1, \ldots, u_d\right) = \alpha\right] \geq 1 - p^{-1},$$

where the probability is taken over all $t_1, \ldots, t_d$ chosen uniformly and independently at random from the elements of $\mathcal{T}$, and over all random choices of the algorithm $\mathcal{A}$.

In order to apply the bound of exponential sums to establish the property of Δ-homogeneous distribution modulo p of a sequence $\mathcal{T}$, we use the following well known result (which, for example, follows immediately from Corollary 3.11 of [20]).

For a real z and an integer m, we use the notation

$$\mathbf{e}_m(z) = \exp(2\pi i z/m).$$

Lemma 2 *Any finite sequence $\mathcal{T}$ of elements of $\mathcal{T}$ is Δ-homogeneously distributed modulo p, with*

$$\Delta = O\left(|\mathcal{T}|^{-1} B \log p\right),$$

where

$$B = \max_{\gcd(c,p)=1} \left| \sum_{t \in \mathcal{T}} \mathbf{e}_p\left(ct\right) \right| .$$

Lemma 3 *Let $g \in \mathbb{F}_p^*$ be of multiplicative order τ modulo p. Then the bound*

$$\max_{\gcd(c,p)=1} \left| \sum_{z=1}^{\tau} \mathbf{e}_p\left(cg^z\right) \right| \ll B(\tau, p),$$

holds, where

$$B(\tau, p) = \min\left\{p^{1/2},\, p^{1/4}\tau^{3/8},\, p^{1/8}\tau^{5/8}\right\}.$$

We also need the following estimate, which follows from Theorem 5.5 of [15].

Lemma 4 *Let Q be a sufficiently large integer. Then, for any $\delta > 0$, there exists $\eta > 0$ such that for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\delta}$ of them, for any $g \in \mathbb{F}_p$ of multiplicative order $\tau \geq p^{\delta}$, the bound*

$$\max_{\gcd(a,p)=1} \left| \sum_{x=0}^{\tau-1} \mathbf{e}_p\left(ag^x\right) \right| = O\left(\tau p^{-\eta}\right)$$

holds.

Proof. For each integer $\tau \geq 1$ and for each prime $p \equiv 1 \pmod{\tau}$ we fix an element $g_{p,\tau}$ of multiplicative order τ. Then Theorem 5.5 of [15] claims that for any $U > 1$ and any integer $\nu \geq 2$, for all primes $p \equiv 1 \pmod{\tau}$ except at most $O(U/\log U)$ of them, the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{\tau-1} \mathbf{e}_p\left(cg_{p,\tau}^x\right) \right| = O\left(\tau p^{1/2\nu^2}\left(\tau^{-1/\nu} + U^{-1/\nu^2}\right)\right)$$

holds. We remark that the value of the above exponential sum does not depend on the particular choice of the element $g_{p,\tau}$.

Taking

$$\nu = \left\lfloor \frac{1}{\delta} \right\rfloor + 1 \qquad \text{and} \qquad U = Q^{1/2+\delta/3},$$

after a simple computation we obtain that there exists some $\eta > 0$, depending only on δ, such that for any fixed $\tau \geq Q^{\delta}$ the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{\tau-1} \mathbf{e}_p\left(cg_{p,\tau}^x\right) \right| \leq \tau^{1-\eta},$$

holds for all except $O(Q^{1/2+\delta/3})$ primes $p \equiv 1 \pmod{\tau}$ in the interval $p \in [Q, 2Q]$. Using Lemma 3, we can see that a similar bound also holds for $\tau \geq Q^{1/3+\delta/3}$. So the total number of exceptional primes p for which the bound of the lemma does not hold for at least one $\tau \geq p^{\delta} \geq Q^{\delta}$ is $O\left(Q^{5/6+2\delta/3}\right)$. Thus for sufficiently large Q we obtain the desired result. $\square$

Combining Lemmas 3 and 4 with the identity

$$\sum_{u \in \mathbb{F}_p^*} \mathbf{e}_p\left(cu^n\right) = \frac{p-1}{\tau} \sum_{x=0}^{\tau-1} \mathbf{e}_p\left(cg^x\right),$$

where $g \in \mathbb{F}_p^*$ is of multiplicative order

$$\tau = \frac{p-1}{\gcd(p-1, n)} \geq (p-1)/n,$$

we obtain the following bound of *Gauss sums*.

Lemma 5 *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$, except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for $n \leq p^{1-\vartheta-\varepsilon}$ the bound*

$$\max_{\gcd(c,p)=1} \left| \sum_{u \in \mathbb{F}_p^*} \mathbf{e}_p\left(cu^n\right) \right| \leq p^{1-\delta},$$

holds.

3 Main Result

We say that a class $\mathcal{M}_n$ of $n \times n$ matrices with entries from $\mathbb{F}_p$ is *homogeneous* if for any $X = (x_{ij})_{i,j=1}^n \in \mathcal{M}_n$ and any $\lambda \in \mathbb{F}_p^*$ we also have $X_\lambda = (\lambda x_{ij})_{i,j=1}^n \in \mathcal{M}_n$.

Let $\mathcal{PER}_{\mathcal{M}_n,k}$ denote an oracle which, given any $X \in \mathcal{M}_n$, outputs $\mathrm{APPROX}_{k,p}(\operatorname{per} X)$.

Theorem 6 *Let $\gamma > 0$ and $\varepsilon > 0$ be arbitrary constants, and let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$*

except for at most $Q^{5/6+\varepsilon}$ *of them. For any homogeneous class of matrices* $\mathcal{M}_n$ *over* F_p *of size* $n \le p^{1-\vartheta-\varepsilon}$ *there exists a probabilistic algorithm running in time polynomial in* n *and* $\log p$ *which for any* $X \in \mathcal{M}_n$*, makes* $O\left((\log p \log\log p/\log\log\log p)^{1/2}\right)$ *calls to the oracle* $\mathcal{PER}_{\mathcal{M}_n,k}$ *with*

$$k = \left\lceil \gamma \left(\frac{\log p \log\log\log p}{\log\log p} \right)^{1/2} \right\rceil$$

and evaluates $\operatorname{per} X$ *correctly with probability at least* $1 - 1/p$*.*

Proof. Given $X \in \mathcal{M}_n$, let us select $\lambda \in \mathbb{F}_p^*$ uniformly at random, compute X_λ and use the oracle $\mathcal{PER}_{\mathcal{M}_n,k}$ with the input X_λ to evaluate

$$\mathrm{APPROX}_{k,p}\left(\operatorname{per} X_\lambda\right) = \mathrm{APPROX}_{k,p}\left(\lambda^n \operatorname{per} X\right).$$

Combining Lemma 2 and Lemma 5 we see that the sequence $(\lambda^n)_{\lambda \in \mathbb{F}_p^*}$ is 2^{-k}-homogeneously distributed modulo p. Now from Lemma 1, we obtain the desired result. □

Corollary 7 *Let* $\gamma > 0$ *and* $\varepsilon > 0$ *be arbitrary constants. Then if there is an algorithm achieving an approximation of* $\mathrm{APPROX}_{k,p}(\operatorname{per} A)$ *with*

$$k = \left\lceil \gamma \left(\frac{\log p \log\log\log p}{\log\log p} \right)^{1/2} \right\rceil$$

to the permanent of an $n \times n$ *symmetric matrix* A *over* $\mathbb{F}_p$*, with* $n \le \frac{\log p}{\log\log p}$*, then* $\mathbf{P}^{\sharp\mathbf{P}} = \mathbf{BPP}$*.*

Proof. We show that the above algorithm can be transformed into a probabilistic algorithm to compute the permanent of symmetric $n \times n$ binary matrices (that is, matrices with 0, 1-entries). The latter problem is $\sharp\mathbf{P}$-complete, as follows from the easy reduction mapping any arbitrary $n \times n$ binary matrix C into the $2n \times 2n$ symmetric matrix

$$D = \begin{bmatrix} 0 & C \\ C^T & 0 \end{bmatrix},$$

whose permanent is the square of the permanent of C, $\operatorname{per} D = (\operatorname{per} C)^2$.

Given any symmetric $n \times n$ binary matrix B, it is obvious that $0 \leq \operatorname{per} B \leq n!$.

Let us set $Q = n^n$, and let us choose n^3 random integers $m \in [Q, 2Q]$. Using the fact that there are at least $cQ/\log Q$ primes in this interval, we have that, for a sufficiently large n, and with probability at least

$$1 - \left(1 - \frac{c}{n \log n}\right)^{n^3} \geq 1 - e^{-2n},$$

one of these n^3 integers is prime. Then we can use one of the probabilistic primality tests to find at least one prime among the selected numbers. Running for each number the Miller–Rabin test n times, see Section 9.5 of [1], and taking into account that for any integer it returns a wrong answer with probability not exceeding 4^{-n}, it turns out that we find a prime with probability at least

$$\left(1 - e^{-2n}\right)\left(1 - n^3 4^{-n}\right) \geq 1 - e^{-n}.$$

By Theorem 6, any approximation algorithm can be transformed into a probabilistic algorithm to compute the residue of $\operatorname{per} B$ modulo p. However, since $0 \leq \operatorname{per} B \leq n! < p$ this residue coincides with the actual value of $\operatorname{per} B$. The thesis now follows by applying a result by Cai et al. [7], who have proved that the existence of a probabilistic algorithm correctly computing the permanent of a matrix for any inverse polynomial fraction of all inputs implies the unlikely collapse $\mathbf{P}^{\sharp\mathbf{P}} = \mathbf{BPP}$. □

4 Remarks

We remark that although the traditional measure for the size of an $n \times n$ matrix X over $\mathbb{F}_p$ is about $n^2 \log p$, some matrices admit a much shorter description. For example, an s-sparse circulant matrix, with only s non-zero entries per row can be described by only $O(s \log np)$ bits. For such matrices it is enough to specify s pairs (m_ν, x_ν), $\nu = 1, \ldots, s$, where m_ν, $1 \leq m_\nu \leq n$, is the position of the νth nonzero entry $x_\nu \in \mathbb{F}_p$ in the first row. In this case, provided that the oracle $\mathcal{PER}_{\mathcal{M}_n,k}$ accepts such a description, the algorithm of Theorem 6 becomes polynomial in $s \log np$.

Using this setting, one can consider an analogue of Theorem 6 for the determinant as well. Indeed, although the determinant is an "easy" function for dense matrices, it is not clear whether for s-sparse circulants it can be

computed in time polynomial in $s \log np$. Moreover, an analogue of Theorem 6 and its modification for matrices with "short description" holds for the much wider class of matrix functions known as *immanants*, whose complexity has been studied, for example, by [5, 6]. Immanants are expressions of the form

$$\operatorname{imm}_\chi X = \sum_{\sigma \in \mathcal{S}_n} \chi(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)},$$

where $\chi : \mathcal{S}_n \to \mathbb{C}$ is an irreducible character of the symmetric group $\mathcal{S}_n$. The trivial character $\chi(\sigma) = 1$ corresponds to the permanent, the alternating character $\chi(\sigma) = \operatorname{sign} \sigma$ corresponds to the determinant.

Our approach can also be used to prove the hardness of modular approximation of several other polynomial functions, such as cycle format polynomials and the factor polynomials (see Section 3.3 of [6]).

References

[1] E. Bach and J. Shallit, *Algorithmic number theory*, MIT Press, 1996.

[2] A. Bernasconi, B. Codenotti, V. Crespi and G. Resta, 'How fast can one compute the permanent of circulant matrices?', *Linear Algebra and its Appl.*, **292** (1999), 15–37.

[3] D. Boneh and R. Venkatesan, 'Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 129–142.

[4] D. Boneh and R. Venkatesan, 'Rounding in lattices and its cryptographic applications', *Proc. 8th Annual ACM-SIAM Symp. on Discr. Algorithms*, ACM, NY, 1997, 675–681.

[5] P. Bürgisser, 'The computational complexity of immanants', *SIAM J. Comp.*, **30** (2000), 1023–1040.

[6] P. Bürgisser, *Completeness and reduction in algebraic complexity theory*, Springer-Verlag, Berlin, 2000.

[7] J.-Y. Cai, A. Pavan and D. Sivakumar, 'On the hardness of permanent', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1563** (1999), 90–99.

[8] B. Codenotti and G. Resta, 'On the permanent of certain circulant matrices', *Algebraic combinatorics and computer science*, Springer–Italia, Milan, 2001, 513–532.

[9] B. Codenotti and G. Resta, 'Computation of sparse circulant permanents via determinants', *Linear Algebra and its Appl.*, 2002 (to appear).

[10] E. El Mahassni, P. Q. Nguyen and I. E. Shparlinski, 'The insecurity of Nyberg–Rueppel and other DSA-like signature schemes with partially known nonces', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2146** (2001), 97–109.

[11] U. Feige and C. Lund, 'On the hardness of computing the permanent of random matrices', *Comp. Compl.*, **6** (1996/1997), 101–132.

[12] M. I. González Vasco and I. E. Shparlinski, 'On the security of Diffie–Hellman bits', *Proc. Workshop on Cryptography and Computational Number Theory*, Singapore 1999, Birkhäuser, 2001, 257–268.

[13] M. I. González Vasco and I. E. Shparlinski, 'Security of the most significant bits of the Shamir message passing scheme', *Math. Comp.*, **71** (2002), 333–342.

[14] M. Jerrum, A. Sinclair and E. Vigoda, 'A polynomial-time algorithm for the permanent of a matrix with non-negative entries', *Electronic Colloq. on Comp. Compl.*, Univ. of Trier, **TR2000-079** (2000), 1–22.

[15] S. V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.

[16] W.-C. W. Li, M. Näslund and I. E. Shparlinski, 'The hidden number problem with the trace and bit security of XTR and LUC', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2442** (2002), 433–448.

[17] N. Linial, A. Samorodinski and A. Wigderson, 'A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents', *Proc. 30th ACM Symp. on Theory of Comp.*, (1998), 644–652.

[18] P. Q. Nguyen and I. E. Shparlinski, 'The insecurity of the Digital Signature Algorithm with partially known nonces', *J. Cryptology*, **15** (2002), 151–176.

[19] P. Q. Nguyen and I. E. Shparlinski, 'The insecurity of the elliptic curve Digital Signature Algorithm with partially known nonces', *Designs, Codes and Cryptography*, (to appear).

[20] H. Niederreiter, *Random number generation and quasi–Monte Carlo methods*, SIAM, Philadelphia, 1992.

[21] I. E. Shparlinski, 'Sparse polynomial approximation in finite fields', *Proc. 33rd ACM Symp. on Theory of Comput.*, Crete, Greece, July 6-8, 2001, 209–215.

[22] I. E. Shparlinski, 'On the generalised hidden number problem and bit security of XTR', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 268–277.

[23] I. E. Shparlinski, 'Security of most significant bits of g^{x^2}', *Inform. Proc. Letters*, **83** (2002), 109–113.

[24] L. G. Valiant, 'Completeness classes in algebra', *Proc 11th ACM Symp. on the Theory of Comput.*, 1979, 249–261.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'