Optimal cycle codes constructed from Ramanujan graphs

Jean-Pierre Tillich* Gilles Zémor†

October 5, 2005

Abstract

We aim here at showing how some known Ramanujan Cayley graphs yield error-correcting codes that are asymptotically optimal in the class of cycle codes of graphs.

The main reason why known constructions of Ramanujan graphs yield good cycle codes is that the number of their cycles of a given length behaves essentially like that of random regular graphs. More precisely we show that for actual constructions of Ramanujan graphs of degree Δ which are bipartite, and for the double cover of known Ramanujan graphs which are not bipartite, the number of cycles of length $2l$ is $\mathcal{O}_\varepsilon(\Delta - 1 + \varepsilon)^{2l}$ (for every $\varepsilon > 0$), which is as about the same as one could expect from a random regular graph of degree Δ. Furthermore, it is possible to show that this property guarantees the highest possible error-probability p that the corresponding cycle codes can sustain, among the class of cycle codes of Δ-regular graphs. This gives a constructive answer to an early problem in coding theory, namely determining what is asymptotically the best possible performance of cycle codes of graphs, when submitted to the binary symmetric channel.

Keywords. Ramanujan Graph, cycle code, error-probability

AMS subject classifications. O5C25, 05C38, 05C80, 11Z05, 68R10, 94A24, 94B25, 94B70

1 Cycle codes of graphs

Let $\boldsymbol{F}_2 = \{0, 1\}$ denote the field on two elements. For any set S denote by 2^S the set of subsets of S. If $\mathbf{x}, \mathbf{y} \in 2^S$, $\mathbf{x}+\mathbf{y}$ will denote the symmetric difference of $\mathbf{x}$ and $\mathbf{y}$. 2^S is in a natural correspondence

*Dept. of Mathematics, University of British Columbia, Vancouver V6T 1Z2, Canada

†Network Dept., Ecole Nationale Supérieure des Télécommunications, 75634 Paris 13, France

with $\boldsymbol{F}_2^s$, the vector space of binary s-tuples where $s = \#S$, and we shall identify subsets of S with their characteristic vectors in $\boldsymbol{F}_2^s$.

Let Γ be a finite graph. Denote by V and E the set of vertices and the set of edges of Γ respectively. Let $v = \#V$ and $n = \#E$ denote the cardinalities of V and E. An edge of Γ is an element of 2^V containing exactly two vertices. For any edge $e \in E$, define its *boundary* $\partial e \in 2^V$ as the union of its endpoints. ∂ is naturally extended to a mapping of 2^E to 2^V, where,

$$\partial : \ \mathbf{x} \mapsto \sum_{e \in \mathbf{x}} \partial e.$$

A (homological) *cycle* is a set of edges with zero boundary. Its connected components correspond to closed paths, and we refer to them as *elementary cycles*. The set of cycles of Γ, denoted by $\mathcal{C}(\Gamma)$ is a linear code (i.e. a vector space) over $\boldsymbol{F}_2$ refered to as the *cycle code* of Γ. If the graph Γ is connected, which we shall always suppose in what follows, $\mathcal{C}(\Gamma)$ has dimension $k = \dim \mathcal{C}(\Gamma) = n - v + 1$. We shall consider from now on only Δ-regular graphs, i.e. graphs such that every vertex has exactly Δ neighbours. In this case, $k = \dim \mathcal{C}(G) = n(1 - 2/\Delta) + 1$. The size of the smallest cycle in Γ is called the *girth* of Γ by graph-theorists and is the *minimum distance* of $\mathcal{C}(\Gamma)$ for coding theorists : denote it by $d(\Gamma)$, or simply d.

Error-probabilities. We are interested in the probability $f_\Gamma(p)$ that a random set of edges $\mathbf{x}$ contains half the edges of some cycle, when $\mathbf{x}$ is obtained by choosing every edge independently with probability p. More precisely, define

$$\begin{array}{rcl} [0,1] & \to & [0,1] \\ p & \mapsto & f_\Gamma(p) = \displaystyle\sum_{\mathbf{x} \in W} p^{|\mathbf{x}|}(1-p)^{n-|\mathbf{x}|} \end{array}$$

where $|\mathbf{x}|$ denotes the weight (cardinality) of $\mathbf{x}$ and where

$$W = \{\mathbf{x} \in 2^E \mid \exists \mathbf{c} \in \mathcal{C}(\Gamma), \mathbf{c} \neq \mathbf{0}, |\mathbf{x} \cap \mathbf{c}| \geq |\mathbf{c}|/2\}.$$

In other words, W is the set of vectors that are closer, for the Hamming distance, to some nonzero codeword (cycle) than to the origin.

From the coding point of view, we are submitting codewords of $\mathcal{C}(\Gamma)$ to the binary symmetric (communication) channel with error-probability p. This means that each transmitted binary symbol is transformed into the complementary symbol independently with probability p. One can assume, by linearity and without loss of generality, that the submitted codeword is the $\mathbf{0}$ vector. The received vector is then some random error vector $\mathbf{x}$, which is decoded by choosing the codeword closest to it for the Hamming distance. Whenever decoding produces a codeword different from $\mathbf{0}$, or a choice between $\mathbf{0}$ and one (or more) other closest codewords, we shall say that a *decoding* (or residual)

error occurs. The probability that a decoding error occurs is therefore exactly the probability that $\mathbf{x} \in W$, i.e. equals $f_\Gamma(p)$.

Cycle codes of graphs were among the first families of graphs to be investigated during the early days of coding theory, see e.g. [10]. They quickly became obsolete because of their poor minimal distance properties, namely for growing n and fixed rate k/n (equivalently for fixed degree Δ), d must be upperbounded by a logarithmic function of n. However, they remain of theoretical interest because they can provide, for fixed rate k/n, infinite families of codes for which $f_{\Gamma_n}(p)$ tends to 0 when $n \to \infty$, for any $p < p_0$, for some fixed p_0. For instance, we have :

Proposition 1 *If (Γ_n) is a family of Δ-regular graphs whose girths satisfy*

$$d(\Gamma_n) \geq c \log_{\Delta-1} n,$$

then $\lim_{n\to\infty} f_{\Gamma_n}(p) = 0$ for any $p < p_0$, where

$$p_0 = \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{(\Delta-1)^{2(1+2/c)}}}\right).$$

Proof
Let Ω_n be a subset of the edge set of Γ_n. If Ω_n contains half the edges of some cycle, then there must exist a vertex x of Γ_n and a path of length $m = \lfloor d/2 \rfloor$ rooted at x with at least half its edges in Ω_n. (To find such a vertex x, travel around the cycle). Consider now that Ω_n is obtained by choosing randomly each edge of Γ_n with independent probability $p < 1/2$. We can upperbound the probability that Ω_n contains half the edges of a cycle by the probability that such a vertex x exists, so that :

$$f_{\Gamma_n}(p) \leq v\Delta(\Delta-1)^{m-1} \sum_{m/2 \leq i \leq m} \binom{m}{i} p^i (1-p)^{m-i}$$

which gives, since $p < 1/2$,

$$f_{\Gamma_n}(p) \leq Cn \left[2(\Delta-1)\sqrt{p(1-p)}\right]^m$$

where C is a constant. It is now straightforward to check that $f_{\Gamma_n}(p) \leq Cn^{-\alpha}$ for some positive α whenever $p < p_0$. □

Infinite families of graphs (Γ_n) satisfying $d \geq c \log_{\Delta-1} n$ were first constructed in [16].

For a family $\mathcal{G} = (\Gamma_n)$ of Δ-regular graphs, denote by

$$\theta(\mathcal{G}) = \sup\{p \mid \lim_{n\to\infty} f_{\Gamma_n}(p) = 0\}.$$

Not so many constructive classes of codes that achieve vanishing residual error probability for positive p are known. Besides constructions that use concatenation [7, 13], one can quote essentially low-density parity check codes, a generalization of cycle codes of graphs, [8], taken up again in [20], and product-type codes originating in [6]. For both these classes of codes it is a difficult problem to determine, for given rate k/n, the largest p for which decoding error probability vanishing with n can be achieved. Hence the motivation for solving one of the remaining open problems for cycle codes of graphs, namely

- determining the largest possible $\theta(\mathcal{G})$ for families of Δ-regular graphs $\mathcal{G} = (\Gamma_n)$
- finding actual constructions of families $\mathcal{G} = (\Gamma_n)$ achieving this value of θ.

In [3] it is proved that for any family of Δ-regular graphs, one must have

$$\theta \leq \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{(\Delta-1)^2}}\right).$$

In this paper we show that some families of known Ramanujan Cayley graphs achieve the above value of θ and in this sense are optimal among the class of cycle codes of graphs.

This will be ensured by estimating the number A_i of cycles of length i of the graphs under consideration and using the following :

Proposition 2 *If $\mathcal{G} = (\Gamma_n)$ is a family of Δ-regular graphs such that*

1. $\lim_{n\to\infty} d(\Gamma_n) = \infty$
2. *for any $\varepsilon > 0$, there exists c_ε such that the number A_i of elementary cycles of length i of any member of $\mathcal{G}$ satisfies*
$$A_i \leq c_\varepsilon(\Delta - 1 + \varepsilon)^i,$$

then

$$\theta(\mathcal{G}) = \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{(\Delta-1)^2}}\right).$$

Proof

Consider That Ω_n is a subset of the edge set of Γ_n obtained by choosing randomly each edge with

independent probability $p \leq 1/2$. Let X_n be the number of subsets of edges of Ω_n that consist of at least half the edges of a cycle. The expected value of X_n is :

$$\mathbf{E}_p(X_n) = \sum_{i \geq d(\Gamma_n)} A_i \sum_{j=i/2}^{i} \binom{i}{j} p^j (1-p)^{i-j}$$

where A_i is the number of elementary cycles of length i. Hence,

$$\mathbf{E}_p(X_n) \leq \sum_{i \geq d(\Gamma_n)} A_i 2^i [p(1-p)]^{i/2}$$

for any $p \leq 1/2$. Therefore,

$$\mathbf{E}_p(X_n) \leq c_\varepsilon \sum_{i \geq d(\Gamma_n)} \left((\Delta - 1 + \varepsilon) 2\sqrt{p(1-p)} \right)^i .$$

It is routinely checked that whenever $p < \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{(\Delta-1+\varepsilon)^2}}\right)$, then $(\Delta - 1 + \varepsilon)2\sqrt{p(1-p)} < 1$, so that $\lim_{n\to\infty} \mathbf{E}_p(X_n) = 0$ whenever $d(\Gamma_n) \to \infty$. And necessarily, if $\lim_{n\to\infty} \mathbf{E}_p(X_n) = 0$ then $\lim_{n\to\infty} f_{\Gamma_n}(p) = 0$. $\square$

Remark. It can be checked easily enough that the expected number of homological cycles of length $2i$ of a randomly chosen Δ-regular bipartite graph is $(\Delta - 1)^{2i}$. Note that this means that random Δ-regular graphs have cycles of constant length. This must be avoided to obtain the conclusion of proposition 2. Hence condition 1 in the proposition, which is satisfied by the Ramanujan graphs we consider.

2 Ramanujan graphs

There are several ways to define the actual explicit constructions of Ramanujan graphs (given in [1, 14, 15, 17, 18]). All these constructions can be described as $q+1$-regular Cayley graphs over $PGL_2(\boldsymbol{F}_{q'})$ or $PSL_2(\boldsymbol{F}_{q'})$, where q and q' are two prime powers, and $\boldsymbol{F}_{q'}$ is the finite field with q' elements.

For our purposes it will be more convenient to use the quaternion description of these graphs. As a matter of fact, by using the latter description we can relate the problem of counting the number of cycles of a given length to the problem of estimating the number of solutions of some diophantine equation.

Basically the construction of those Ramanujan graphs is done in two steps.

1. The first step consists of constructing the $q+1$-regular infinite tree in an arithmetic way by using

quaternions.
2. One obtains finite Ramanujan graphs from this tree by taking suitable finite quotients of this tree which do not create small cycles.

Let us see these constructions in more detail.

The construction of the infinite tree of degree $q+1$

The construction of the infinite tree starts by considering the following set of quaternions $\mathcal{S} = \mathcal{A}\mathbf{1} + \mathcal{A}\boldsymbol{i} + \mathcal{A}\boldsymbol{j} + \mathcal{A}\boldsymbol{ij}$, where $\mathcal{A}$ is an euclidean domain which will be either $\mathbb{Z}$ or $\boldsymbol{F}_q[X]$. We will denote by $\overline{x}$ the conjugate of the element $x \in \mathcal{S}$, and by $N(x) = x\overline{x} \in \mathcal{A}$ the norm of x. Then a prime π is chosen in $\mathcal{A}$: this is a prime number equal to q when $\mathcal{A} = \mathbb{Z}$, and X when $\mathcal{A} = \boldsymbol{F}_q[X]$ for odd q, and $X+1$ for even q.

The basic step consists of setting up a set of $q+1$ quaternions $\alpha_1, \alpha_2, \cdots, \alpha_{q+1}$ of norm π such that
1. every quaternion α of norm π^n has a unique factorization

$$\alpha = u\pi^r \alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_m}$$

where u is a unit (an element of norm 1 here), and $2r+m=n$, and where the product of two consecutive terms of the product α_{i_j} and $\alpha_{i_{j+1}}$ never belongs to $\mathcal{A}$.
2. for every α_i, $\overline{\alpha_i}$ is equal to some $\pm\alpha_j$

We refer to [15, 17, 18, 19] to see how this set of quaternions is obtained. This set now enables us to construct the infinite $q+1$ regular tree as a Cayley graph. The group G from which this graph is constructed is just the set of quaternions generated by the α_i's and we identify the quaternions which differ by a multiplication of some $\pm\pi^i$. Let us denote by $[\alpha]$ the equivalence class associated to α. This group is clearly generated by the $[\alpha_i]$'s and the inverse of $[\alpha_i]$ is $[\alpha_j]$ where α_j is the quaternion such that $\alpha_j = \pm\overline{\alpha_i}$ (since $[\alpha_i][\pm\overline{\alpha_i}] = [\pm\alpha_i\overline{\alpha_i}] = [\pm\pi] = [1]$). That the infinite Cayley graph over G with generator set $[\alpha_1], [\alpha_2], \cdots, [\alpha_{q+1}]$ is indeed the $q+1$-regular infinite tree is just a consequence of the fact that every quaternion of norm π^n has a unique factorization over the α_i's.

We have depicted such an example in figure 1, when there are 3 generators $[\alpha_1], [\alpha_2], [\alpha_3]$ and we have assumed that $\overline{\alpha_1} = \alpha_2$ and $\overline{\alpha_3} = \alpha_3$, in other words $[\alpha_1]^{-1} = [\alpha_2]$ and $[\alpha_3]^{-1} = [\alpha_3]$.

The finite Cayley graph

We obtain our Ramanujan graph by taking a finite quotient of this infinite tree, and this quotient will be realized as a Cayley graph by choosing a suitable normal subgroup H of G of finite index. One selects first a prime π' of $\mathcal{A}$ which satisfies certain conditions (for more details see the

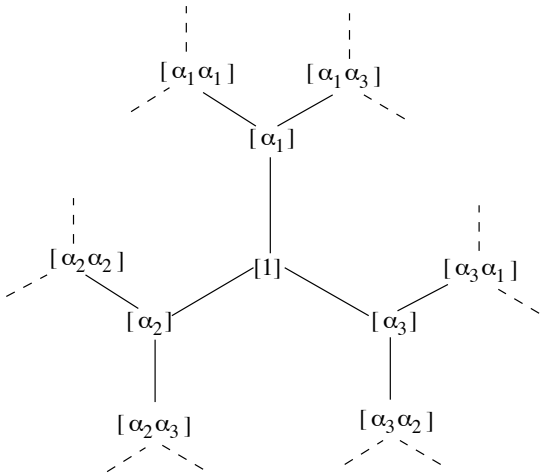

Figure 1: the infinite tree

following section). H is defined as the set of classes $[\alpha] = [a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{ij}]$ for which a_1, a_2, a_3 are multiples of π'. This set is clearly a normal subgroup for it can be seen as the kernel of the homomorphism ϕ

$$\begin{aligned} \phi : G &\rightarrow \mathbb{H}(\mathcal{A}/\pi'\mathcal{A})^*/Z \\ [\alpha] &\mapsto (\alpha \bmod \pi')Z \end{aligned}$$

where $\mathbb{H}(\mathcal{A}/\pi'\mathcal{A})$ denotes the ring of quaternions with entries in the field $\mathcal{A}/\pi'\mathcal{A}$, $\mathbb{H}(\mathcal{A}/\pi'\mathcal{A})^*$, the invertible elements of this ring, and Z its central subgroup, which is $\{a \in \mathcal{A}/\pi'\mathcal{A} \mid a \neq 0\}$.

One of the attractive features of this way of constructing a Cayley graph is that the study of the number of cycles of a given length can now be expressed as a problem in number theory.

Counting Cycles of a given length

In order to bound the number of cycles of a given length in the finite Cayley graph which has been constructed we can observe that

Fact 1 *The number of elementary cycles of length l in a graph is less than the number of non-backtracking closed walks of length l. In an undirected Cayley graph this is less than the number of vertices v of the graph times the number of non-backtracking walks of length l which start at the identity of the group and which go back to this vertex.*

Fact 2 *A non-backtracking walk of length l corresponds in the case described above to a sequence $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_l}$ such that no consecutive terms are conjugate, and this non-backtracking walk returns*

to its starting point (is closed) if and only if the product $[\alpha_{i_1}][\alpha_{i_2}]\cdots[\alpha_{i_l}]$ *is an element of the normal subgroup* H*, or what amounts to the same thing, iff the product* $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_l}$ *is of the form* $a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{ij}$ *where* a_1, a_2, a_3 *are multiples of the prime* π' *which defines* H*.*

Let us notice now that the norm is multiplicative, and that this implies that the norm of a product $\alpha_{i_1}\alpha_{i_2}\cdots\alpha_{i_l}$ is π^l . Hence :

Fact 3 *The number of non-backtracking closed walks of length* l *is less than*

$$v \,\#\left\{(a_0, a_1, a_2, a_3) \in \mathcal{A}^4 | N(a_0 + ra_1\boldsymbol{i} + ra_2\boldsymbol{j} + ra_3\boldsymbol{ij}) = \pi^l\right\}$$

The norm of a quaternion $a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{ij}$ is a quadratic form in (a_0, a_1, a_2, a_3), and all that we need now, is a tool bounding the number of solutions in $\mathcal{A}$ of a certain quadratic equation. There are several methods which can be employed to estimate the number of solutions of the quadratic equation which arises in our case. The most precise one, which uses the work of Drinfeld, Eichler, and Igusa (see [4, 5, 12]) does not give enough information on the number of "small" cycles. We use instead very simple (and classical) arguments (see [9] for example) to bound the number of solutions of such equations, and this is obtained by the following lemma

lemma 1 *Let* $\mathcal{A}$ *be the ring* $\mathbb{Z}$ *or* $\boldsymbol{F}_q[X]$*,* $R = \mathcal{A} + \mathcal{A}\boldsymbol{i}$*, where* $\boldsymbol{i}$ *is an algebraic integer of degree* 2 *over* $\mathcal{A}$ *(i.e* $\boldsymbol{i}$ *does not belong to* $\mathcal{A}$ *and satifies an equation* $\boldsymbol{i}^2 + a\boldsymbol{i} + b = 0$*, with* $a, b \in \mathcal{A}$*). Let* $\overline{\boldsymbol{i}}$ *be the other solution of this equation, and define the following automorphism of* R*, by* $\overline{x + y\boldsymbol{i}} = x + y\overline{\boldsymbol{i}}$*, and the multiplicative morphism* N *"the norm" from* R *to* $\mathcal{A}$ *by* $N(x) = x\overline{x}$*. If* R *is a unique factorization domain, then the number of solutions of the equation* $N(x) = c$ *(the unknown is* x*, and* c *is a given element of* $\mathcal{A}$*) is* $\mathcal{O}_\delta(c^\delta)$ *if* $\mathcal{A} = \mathbb{Z}$*, and* $\mathcal{O}_{\delta(}q^{\delta \deg c})$ *if* $\mathcal{A} = \boldsymbol{F}_q[X]$*, and this for every* $\delta > 0$*.*

See the appendix for a proof.

The bipartite cover

Actually, for the graphs we consider, we are able to give rather tight upper bounds on the cardinality of the set in fact 3, i.e. on the number of non-backtracking closed walks, only when their length l is even. This approach works well when the Cayley graph is bipartite, because there are no odd cycles. When this graph is not bipartite, we shall move around this difficulty by considering its bipartite *double cover*.

Definition Let $\Gamma(V, E)$ be a graph with set of vertices V, and set of edges E. Its *double cover* $\hat{\Gamma}$ is defined by the set of vertices $\hat{V} = V \times \{0, 1\}$, and the set of edges $\hat{E} = \{\{(x, 0), (y, 1)\} \text{ for } \{x, y\} \in E\}$.

An attractive feature of this double cover is

Fact 4 *The double cover of a graph* Γ *is*
– *connected iff* Γ *is connected and non bipartite,*
– *bipartite and has therefore only cycles of even length. Furthermore, the projection*

$$\begin{array}{ccc} \hat{V} & \longrightarrow & V \\ (x, i) & \mapsto & x \end{array}$$

for $i = 0, 1$ *induces a two-to-one correspondence between the non-backtracking closed walks of* $\hat{\Gamma}$ *and the non-backtracking closed walks of* even length *of* Γ.

By taking double covers if need be, we shall look therefore for graphs that satisfy the conditions of proposition 2 among bipartite graphs.

3 Estimation of the number of cycles in some Ramanujan graphs

We are going to show in this section that some of the Ramanujan graphs constructed in [15, 17, 18] meet the hypotheses of proposition 2, which implies that the associated families of cycle codes are optimal. We do not give all the steps involved in the construction of these graphs, and merely refer to [15, 17, 18, 19] for further details. A rough description in the spirit of the general presentation of section 2 will suffice for our needs. The parameters of these graphs which are relevant to counting cycles are gathered in tableau format in figure 2.

3.1 The Ramanujan graphs constructed by Margulis and Lubotzky, Philipps, Sarnak

They correspond to the choice $\mathcal{A} = \mathbb{Z}$. We denote these graphs by $\mathcal{X}^{p,q}$, where q denotes the odd prime number chosen for π, and p the odd prime number chosen for π'. Now, upperbounding the number of vertices v by p^3, Fact 3 translates to

Fact 3' *The number of non-backtracking closed walks of length* l *in* $\mathcal{X}^{p,q}$ *is less than*

$$p^3 \, \#\{(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 | a_0^2 + p^2 a_1^2 + p^2 a_2^2 + p^2 a_3^2 = q^l\}.$$

	graphs constructed in [15, 17]	graphs constructed in [18]	graphs constructed in [18]
$\mathcal{A}$	$\mathbb{Z}$	$\boldsymbol{F}_q[X],\ q=p^n,$ p odd prime	$\boldsymbol{F}_{2^n}[X]$
$\mathbb{H}(\mathcal{A})$ $=$ $\mathcal{A}+\mathcal{A}\boldsymbol{i}+\mathcal{A}\boldsymbol{j}+\mathcal{A}\boldsymbol{ij}$	$\boldsymbol{i}^2=\boldsymbol{j}^2=(\boldsymbol{ij})^2=-1$ $\boldsymbol{ij}=-\boldsymbol{ji}$	$\boldsymbol{i}^2=\eta$ η is not a square in $\boldsymbol{F}_q$ $\boldsymbol{j}^2=X-1, \boldsymbol{ij}=-\boldsymbol{ji}$	$\boldsymbol{i}^2=\boldsymbol{i}+\eta,$ η is such that $X^2+X+\eta$ is irreducible over $\boldsymbol{F}_{2^n}$, $\boldsymbol{j}^2=X, \boldsymbol{ij}=\boldsymbol{ji}+\boldsymbol{j}$
$\overline{\alpha}$, $\alpha=a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{ij}$	$a-b\boldsymbol{i}-c\boldsymbol{j}-d\boldsymbol{ij}$	$a-b\boldsymbol{i}-c\boldsymbol{j}-d\boldsymbol{ij}$	$(a+b)+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{ij}$
$N(\alpha)$	$a^2+b^2+c^2+d^2$	$a^2-\eta b^2$ $-(X-1)(c^2-\eta d^2)$	$a^2+\eta b^2+ab$ $+X(c^2+\eta d^2+cd)$
π	odd prime number q	X	$X+1$
π'	odd prime number p	irreducible polynomial $g(X)\in\boldsymbol{F}_q[X]$	irreducible polynomial $g(X)\in\boldsymbol{F}_{2^n}[X]$
degree of the graph	$q+1$	$q+1$	2^n+1
Number of vertices of the Ramanujan graph	$p(p^2-1)$ if $\left(\frac{q}{p}\right)=-1$ $\frac{p(p^2-1)}{2}$ if $\left(\frac{q}{p}\right)=1$	$q^{3d}-q^d$ if $\left(\frac{X}{g(X)}\right)=-1$ $\frac{q^{3d}-q^d}{2}$ if $\left(\frac{X}{g(X)}\right)=1$ $d=\deg g(X)$	$2^{3nd}-2^{nd}$ $d=\deg g(X)$
bipartite	yes if $\left(\frac{q}{p}\right)=-1$ no if $\left(\frac{q}{p}\right)=1$	yes if $\left(\frac{X}{g(X)}\right)=-1$ no if $\left(\frac{X}{g(X)}\right)=1$	never

Figure 2: Constructions of Ramanujan graphs : There are some additional constraints on π' which are not given here. We refer to [15, 17, 18] for the missing details.

By using lemma 1 it is straightforward to obtain a rather tight upper bound on the number of solutions of this diophantine equation when the length of the cycles is *even*.

lemma 2 *The number of non-backtracking closed walks of length* $2l$ *in* $\mathcal{X}^{p,q}$ *is* $\mathcal{O}_\varepsilon(q+\varepsilon)^{2l}$ *for every* $\varepsilon>0$.

Proof

Assume that $a_0^2+p^2a_1^2+p^2a_2^2+p^2a_3^2=q^{2l}$, then $a_0^2\equiv q^{2l} \bmod p^2$, and thus $a_0\equiv\pm q^l \bmod p^2$ Therefore there at most $\lceil 4q^l/p^2\rceil$ choices for a_0. Since $p^2a_1^2<q^{2l}$, there are at most $\lceil 2q^l/p\rceil$ choices for a_1.

For fixed a_0, a_1, the number of choices we have for the couple (a_2, a_3) is not very large, because $a_2^2 + a_3^2$ should be equal to $\frac{q^{2l} - a_0^2 - p^2 a_1^2}{p^2}$ which is a number smaller than $\frac{q^{2l}}{p^2}$, and from lemma 1 the number of couples (a_2, a_3) which satisfy this inequality is $\mathcal{O}_\varepsilon(q^{2l}/p^2)^\varepsilon$.

Therefore the total number of solutions is less than

$$\lceil 4q^l/p^2 \rceil \lceil 2q^l/p \rceil \mathcal{O}_\varepsilon(q^{2l}/p^2)^\varepsilon = \frac{1}{p^3}\mathcal{O}_\varepsilon(q^{2l(1+\varepsilon)}).$$

We conclude by applying fact 3'. □

Those graphs $\mathcal{X}^{p,q}$ are bipartite if and only if q is not a quadratic residue modulo p, and have in this case only cycles of even length whose numbers can be bounded with the previous lemma. Moreover in this case the graphs $\mathcal{X}^{p,q}$ have a very large girth which is $\frac{4}{3}\log_q(p(p^2-1)) + \mathcal{O}(1)$. When q is a quadratic residue modulo p, the graph is not bipartite, but its double cover $\hat{\mathcal{X}}^{p,q}$ has still a large girth, namely $\frac{4}{3}\log_q(p(p^2-1)) + \mathcal{O}(1)$.

Remarks

1. The key fact in lemma 2 has been observed in another setting by G. Davidoff and P. Sarnak too (see [2]).

2. We wish to emphasise here that the results on the girth of $\mathcal{X}^{p,q}$ in the non bipartite case which can be found in the literature give only the lower bound $\frac{2}{3}\log_q(p(p^2-1))$, so the result we invoque here shows that in some sense we can "improve" substantially these graphs by taking their double cover. We justify this by the fact that the double cover has only cycles of even length, and that these project on $\mathcal{X}^{p,q}$ to either cycles of the same even length or to cycles of odd length half as long. The point is that the proof used in [15] for example, to show that the girth in the bipartite case is bigger than $\frac{4}{3}\log_q(p(p^2-1))$ depends only on the fact that a cycle of even length cannot be shorter than this quantity, and therefore also gives a lower bound on the length of the shortest cycle of even length when the graph is not bipartite. That the girth is indeed $\frac{4}{3}\log_q(p(p^2-1)) + \mathcal{O}(1)$ follows from a straightforward generalization of results given in [17].

This leads to the the following result by upperbounding the number of vertices v by $2p^3$, applying fact 1, and using the discussion given in the previous section under the heading "The bipartite cover", together with proposition 2.

Theorem 1 *Let q be a fixed prime. Let $\mathcal{X}_q = (\mathcal{X}^{p,q})$ be the family of those $\mathcal{X}^{p,q}$ for which* $\left(\frac{q}{p}\right) =$

-1. *Let* $\hat{\mathcal{X}}_q = (\hat{\mathcal{X}}^{p,q})$ *be the family of those* $\hat{\mathcal{X}}^{p,q}$ *for which* $\left(\frac{q}{p}\right) = 1$. *Then*

$$\theta(\mathcal{X}_q) = \theta(\hat{\mathcal{X}}_q) = \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{q^2}}\right)$$

3.2 The case $\mathcal{A} = \boldsymbol{F}_q[X]$, q odd prime power

The corresponding Ramanujan graphs have been constructed by Morgenstern (see [18]) and are regular of degree $q+1$. From now on, we consider such a graph obtained by choosing $\pi' = g(X)$ an irreducible polynomial of degree k.

By using fact 3 given in section 2 and by using the fact that the groups over which these finite Cayley graphs are defined have less than q^{3k} elements, we obtain that the number $\mathcal{N}_{2l}$ of non-backtracking closed walks of length $2l$ satisfies

$$\begin{aligned} \mathcal{N}_{2l} &\leq q^{3k} \# \left\{(a,b,c,d) \in (\boldsymbol{F}_q[X])^4 | N(a + gb\boldsymbol{i} + gc\boldsymbol{j} + gd\boldsymbol{ij}) = X^{2l}\right\} \\ &\leq q^{3k} \# \left\{(a,b,c,d) \in (\boldsymbol{F}_q[X])^4 | a^2 - \eta b^2 g^2 + (X-1)g^2(\eta d^2 - c^2) = X^{2l}\right\} \end{aligned} \quad (1)$$

To obtain an estimation of the number of solutions of this equation, we use an upper bound on the number of solutions in $\boldsymbol{F}_q[X]$ of the equation $a^2 - \eta b^2 = P$, where the unknowns are a, b, and P is a given polynomial of degree l. For that purpose we use the classical method which consists of studying the ring $R = \boldsymbol{F}_q[X] + \boldsymbol{F}_q[X]\boldsymbol{i}$. The crucial property of this ring is

lemma 3 $R = \boldsymbol{F}_q[X] + \boldsymbol{i}\boldsymbol{F}_q[X]$ *is an euclidean domain.*

Proof Let $\phi(a + b\boldsymbol{i}) = \deg\left((a + b\boldsymbol{i})(\overline{a + b\boldsymbol{i}})\right) = \deg(a^2 - \eta b^2)$. Since $a^2 - b^2\eta = 0$ implies $a = b = 0$, for $a, b \in \boldsymbol{F}_q[X]$, we deduce that $\phi(\alpha)$ is nonnegative for all $\alpha \neq 0$, and this combined with the relation $\phi(\alpha\beta) = \phi(\alpha) + \phi(\beta)$ shows that R is a domain. To show that R is euclidean it remains to prove that for all α and β in R such that $\phi(\alpha) \geq \phi(\beta)$, there exists a γ in R such that $\phi(\alpha - \gamma\beta) < \phi(\beta)$ or $\alpha = \beta\gamma$.

Let $a + b\boldsymbol{i} = \alpha\overline{\beta}$ and $t = \beta\overline{\beta}$. Carry out the usual euclidean division over $\boldsymbol{F}_q[X]$ of a and b by t : $a = q_1 t + r_1$, $b = q_2 t + r_2$, with $\deg(r_1), \deg(r_2) < \deg(t)$. We claim that we can choose $\gamma = q_1 + q_2\boldsymbol{i}$.

This follows from

$$\begin{aligned}\phi(\alpha-\beta\gamma)+\phi(\overline{\beta}) &= \phi(\alpha\overline{\beta}-\beta\overline{\beta}\gamma)\\ &= \phi(a+b\boldsymbol{i}-t(q_1+q_2\boldsymbol{i}))\\ &= \phi(r_1+r_2\boldsymbol{i})\\ &< 2\deg(t)=\phi(\beta)+\phi(\overline{\beta})\end{aligned}$$

Hence $\phi(\alpha-\beta\gamma)<\phi(\beta)$. This calculation is valid as long as either r_1 or r_2 is different from 0. We handle the case $r_1=r_2=0$ by noticing that in such a case $\alpha\overline{\beta}=a+b\boldsymbol{i}=t\gamma=(\beta\overline{\beta})\gamma=(\beta\gamma)\overline{\beta}$. Therefore $\alpha=\beta\gamma$. □

The ring R is therefore an unique factorization domain. The units of R are exactly the invertible elements of R, which is the set $I=\boldsymbol{F}_q+\boldsymbol{F}_q\boldsymbol{i}-\{0\}$. By using lemma 1 we obtain that the number of solutions (x,y) in $\boldsymbol{F}_q[X]\times\boldsymbol{F}_q[X]$ of the equation $x^2-\eta y^2=P$, where P is some given polynomial of $\boldsymbol{F}_q[X]$ is

$$\mathcal{O}_\varepsilon(q^{\varepsilon\deg P}) \tag{2}$$

From this we can give an upper bound on the number of solutions (a,b,c,d) of

$$a^2-\eta b^2g^2+(X-1)g^2(\eta d^2-c^2)=X^{2l}$$

by noticing that

- $\deg\left(a^2-\eta b^2g^2+(X-1)g^2(\eta d^2-c^2)\right)$
  $=\max\left(2\deg a,\ 2(k+\deg b),\ 2(k+\deg c)+1,\ 2(k+\deg d)+1\right)$,
  and so $l-k\geq\deg(b)$, there are no more than q^{l-k+1} choices for b. The equality on the degree makes use of
  $$x^2-\eta y^2=0 \text{ iff } x=y=0$$
  for $x,y\in\boldsymbol{F}_q$, and therefore $\deg(a^2-b^2\eta)=2\max(\deg a,\deg b)$ for $a,b\in\boldsymbol{F}_q[X]$.
- $a^2\equiv x^{2l}\pmod{g^2}$, and therefore $a\equiv\pm X^l\pmod{g^2}$, thus a can not take on more than $2q^{l-2k+1}$ different values (a is of degree l at most).
- Once a and b are chosen ηd^2-c^2 has to be equal to some polynomial of degree at most $2l-2-2k$ and from (2) we deduce that the number of choices left for (c,d) is $\mathcal{O}_\varepsilon(q^{\varepsilon(2l-2-2k)})$

This yields that the number of non backtracking closed walks of length $2l$ of our Ramanujan graph is $\mathcal{O}_\varepsilon(q+\varepsilon)^{2l}$ (for every $\varepsilon>0$). We now have to treat two cases separately

– either our graph is bipartite (this is if X is not a quadratic residue modulo $g(X)$). The girth of our graph is in this case larger than $4/3 \log_q \left(\frac{q^{3\deg(g)} - q^{\deg(g)}}{2} \right) + 1$ (see theorem 4.1.3 of [18]).
– or our graph is not bipartite (if X is a quadratic residue modulo $g(X)$). Then one can prove easily (by using the argument given in the proof of the lower bound on the girth of these graphs, in theorem 4.13 in [18]) that the bipartite cover of our graphs has a girth which is greater than $4/3 \log_q \left(\frac{q^{3k} - q^k}{2} \right) + 1$ too. We can now conclude by using proposition 2 :

Theorem 2 *Let $\mathcal{X}^{g,q}$ be the Ramanujan graph of degree $q+1$ considered in this section obtained from the choice $\pi' = g(X)$. Let $\mathcal{X}_q$ be the family of graphs $\mathcal{X}^{g,q}$ which are bipartite, and $\mathcal{Y}_q$ be the family of double covers $\hat{\mathcal{X}}^{g,q}$ of all graphs $\mathcal{X}^{g,q}$ which are not bipartite.*

$$\theta(\mathcal{X}_q) = \theta(\mathcal{Y}_q) = \frac{1}{2} \left(1 - \sqrt{1 - \frac{1}{q^2}} \right).$$

3.3 The case of $\mathcal{A} = \boldsymbol{F}_{2^n}[X]$

The corresponding Ramanujan graphs have been constructed by Morgenstern (see [18]) and are regular of degree $2^n + 1$. From now on we consider such a graph obtained by choosing $\pi' = g(X)$ an irreducible polynomial of degree k. We let $q = 2^n$ and we denote this graph by $\mathcal{X}^{g,q}$

By using fact 3 given in section 2 we see that the number $\mathcal{N}_{2l}$ of non-backtracking closed walks of length $2l$ of these graphs $\mathcal{X}^{g,q}$ verifies :

$$\begin{aligned} \mathcal{N}_{2l} &\leq q^{3k} \ \# \left\{ (a,b,c,d) \in (\boldsymbol{F}_q[X])^4 | N(a + gb\boldsymbol{i} + gc\boldsymbol{j} + gd\boldsymbol{ij}) = (X+1)^{2l} \right\} \\ &\leq q^{3k} \ \# \left\{ (a,b,c,d) \in (\boldsymbol{F}_q[X])^4 | a^2 + gab + \eta b^2 g^2 + Xg^2(c^2 + cd + \eta d^2) = (X+1)^{2l} \right\} \end{aligned} \quad (3)$$

We proceed as for the graphs of odd degrees :
we obtain first an estimation of the number of solutions in $\boldsymbol{F}_q[X]$ of the equation $a^2 + b^2\eta + ab = P$, where the unknowns are a, b, and P is a given polynomial. It can be shown in a similar way as lemma 3 that $R = \boldsymbol{F}_q[X] + \boldsymbol{i}\boldsymbol{F}_q[X]$ is an euclidean domain (the only difference being that we use this time the remark $a^2 + \eta b^2 + ab = 0$ iff $a = b = 0$ for $a, b \in \boldsymbol{F}_{2^n}[X]$). Hence by lemma 1 the number of solutions of the aforementioned equation is $\mathcal{O}_\varepsilon(q^{\varepsilon \deg(P)})$ for all $\varepsilon > 0$. This yields the upper bound which holds for every $\varepsilon > 0$,

$$\mathcal{N}_{2l} < \mathcal{O}_\varepsilon \left((q+\varepsilon)^{2l} \right).$$

It can be shown that the girth of the bipartite cover $\hat{\mathcal{X}}^{g,q}$ is not less than $\frac{4}{3}\log_q(q^{3\deg(g)} - q^{\deg(g)})$ (by using the same proof technique as in theorem 4.13 of [18] and by using the fact that there are only cycles of even length). We conclude as before.

Theorem 3 *If $\hat{\mathcal{Y}}_q$ is the family $\hat{\mathcal{Y}}_q = (\hat{\mathcal{X}}^{g,q})$, then*

$$\theta(\hat{\mathcal{Y}}_q) = \frac{1}{2}\left(1 - \sqrt{1 - \frac{1}{q^2}}\right).$$

Acknowledgment : We wish to thank the referees for their help.

APPENDIX : Proof of the Main Lemma

In this section we prove lemma 1.

Recall here a few facts about unique factorization domains :
- there exists a subset E of the unique factorization domain R, called the units, which is the set of elements of R which divide every other element of the domain. In our case this coincides with the set of elements of R of norm a unit of $\mathcal{A}$. These units define an equivalence relation over the domain : two elements x and y are said to be *associated* if and only if there exists a unit u such that $x = yu$.
- there exists a subset Π of elements of the domain called the *primes*, i.e the subset of elements not in E which are not a product of two non-units elements. The set of associated elements to a prime is a set of prime elements, and let us choose for each such class a representative element in an arbitrary way.

In this case every element of the unique factorization domain can be written uniquely (up to re-ordering the factors) as:

$$up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$$

where the p_i's are representative elements of primes, and u is a unit.

In our case we will distinguish between sets of associated primes which contain conjugate pairs of primes, and sets of associated primes which do not contain such conjugate pairs of primes. In what follows
- u will always denote a unit,
- q_i will always denote a representative of a set of associated primes which contains a conjugate pair of primes,
- and p_i a representative of a set of associated primes which does not contain conjugate pairs of

prime. We will choose the p_i's such that every $\overline{p_i}$ is a representative prime of a set of associated primes too.

Let us factorize :

$$c = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \overline{p_1}^{\beta_1} \overline{p_2}^{\beta_2} \cdots \overline{p_m}^{\beta_m} q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_n^{\gamma_n}$$

(where some of the powers can be 0) Since c is in $\mathcal{A}$, $\overline{c}$ is in $\mathcal{A}$, and by the unicity of factorization into primes we get that $\alpha_i = \beta_i$, for every i. If there exists $x \in R$ such that $x\overline{x} = c$, then we can factorize x and $\overline{x}$ by using the same primes p_i's, the $\overline{p_i}$'s and the q_i's.

$$x = u' p_1^{\alpha'_1} p_2^{\alpha'_2} \cdots p_m^{\alpha'_m} \overline{p_1}^{\beta'_1} \overline{p_2}^{\beta'_2} \cdots \overline{p_m}^{\beta'_m} q_1^{\gamma'_1} q_2^{\gamma'_2} \cdots q_n^{\gamma'_n}$$

And therefore

$$\overline{x} = u'' \overline{p_1}^{\alpha'_1} \overline{p_2}^{\alpha'_2} \cdots \overline{p_m}^{\alpha'_m} p_1^{\beta'_1} p_2^{\beta'_2} \cdots p_m^{\beta'_m} q_1^{\gamma'_1} q_2^{\gamma'_2} \cdots q_n^{\gamma'_n}$$

Due to the unicity of factorization into primes, we obtain that for every i

$$\alpha'_i + \beta'_i = \alpha_i \text{ and } \gamma_i = 2\gamma'_i \tag{4}$$

Hence the number of solutions of the equation $x\overline{x} = c$ is equal to the number of ways of choosing an x whose factorization satisfies the conditions (4), the only choice is in fact the choice of u and the choice of the α'_i in $\{0, 1, \cdots, \alpha_i\}$. In order to get an upper bound on this number let $c' = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \overline{p_1}^{\beta_1} \overline{p_2}^{\beta_2} \cdots \overline{p_m}^{\beta_m} = (p_1\overline{p_1})^{\alpha_1} (p_2\overline{p_2})^{\alpha_2} \cdots (p_m\overline{p_m})^{\alpha_m}$ and let us notice that the number of choices for the α'_i's is exactly the number of ways of choosing $y = (p_1\overline{p_1})^{\alpha'_1} (p_2\overline{p_2})^{\alpha'_2} \cdots (p_m\overline{p_m})^{\alpha_m}$ which divide c'. Since c' and y are in $\mathcal{A}$ this coincides with the number of divisors (in $\mathcal{A}$) of the element c' – where we do not not distinguish between divisors which differ by a multiplication of an invertible element of $\mathcal{A}$. This number of divisors is $d(c')$ in the case $\mathcal{A} = \mathbb{Z}$, that is the number of positive integers dividing c', and is equal to the number of polynomials whose leading coefficient is 1 which divide c', when $\mathcal{A} = \boldsymbol{F}_q[X]$. From Theorem 315 in chapter $XVIII$ of [11] we get an upper bound on $d(c')$ of the form $O_\delta(c'^\delta)$ for all $\delta > 0$, and we deduce from that the number of solutions s of the equation $x\overline{x}$ verifies (for every $\delta > 0$)

$$\begin{aligned} s &= \#E \; d(c') \\ &= 4d(c') \\ &= \mathcal{O}_\delta(c^\delta) \end{aligned}$$

We have similar results when $\mathcal{A} = \boldsymbol{F}_q[X]$. In this case $E = \{u + \boldsymbol{i}v | u, v \in \boldsymbol{F}_q, (u, v) \neq (0, 0)\}$, therefore $\#E = q^2 - 1$, and the number of divisors of c', is $O_\delta(q^{\delta \deg c'})$. This is obtained by a straightforward generalisation of Theorem 316 in [11] to polynomials :
if a multiplicative function $f : \boldsymbol{F}_q[X] \mapsto \mathbb{R}$ satisfies $f(p^m) \to 0$ for every irreducible polynomial p

when $m \deg(p) \to \infty$*, then* $f(a) =\to 0$ *when* $\deg(a) \to \infty$.
We let $f(x) = q^{-\delta \deg(x)} d(x)$ which is clearly multiplicative, and satisfies $f(p^m) = (m+1)q^{-\delta m \deg p} \to 0$ as $m \deg p \to \infty$ for an irreducible polynomial p. We can therefore apply the aforementioned generalization and deduce $f(a) = \mathcal{O}(1)$ and therefore $d(a) = \mathcal{O}_\delta(q^{\delta \deg(a)})$.

References

[1] P. Chiu. Cubic Ramanujan graphs. *Combinatorica*, 12(3):275–285, 1992.

[2] G. Davidoff and P. Sarnak An elementary approach to Ramanujan graphs. Preprint.

[3] L. Decreusefond and G. Zémor. On the error-correcting capabilities of cycle codes of graphs. To appear in *Combinatorics, Probability & Computing*.

[4] V. G. Drinfeld. The proof of Peterson's conjecture for $GL(2)$ over global fields of characteristic p. *Functional Analysis and its Applications*, 22:28–43, 1988.

[5] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die kongruent Zeta Funktion. *Archiv. der Math.*, 5:355–366, 1954.

[6] P. Elias Error-free coding *IRE Trans. on Inf. Theory*, IT-4 29–37, 1954.

[7] G. D. Forney. *Concatenated Codes*. M.I.T. Press, Cambridge, Mass. 1966.

[8] R. G. Gallager Low-density parity check codes. *IRE Trans. on Inf. Theory*, IT-8, 21–28, 1962.

[9] E. Grosswald. *Representation of integers as sum of squares*. Springer Verlag, 1985.

[10] S. L. Hakimi and J. G. Bredeson. Graph theoretic error-correcting codes. *IEEE Trans. on Inf. Theory*, IT-14, 584–591, 1968.

[11] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford Press, 1960.

[12] J. Igusa. Fibre systems of Jacobian varieties III. *Amer. Journal*, 81:453–476, 1959.

[13] J. Justesen. A class of asymptotically good algebraic codes. *IEEE Trans. on Inf. Theory*, IT-18, 652–656, 1972.

[14] A. Lubotsky. *Discrete groups, expanding graphs, and invariant measures*. Lectures Notes, U. Oklahoma. Norman, 1989.

[15] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[16] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes *Combinatorica*, 2(1):71–78, 1982.

[17] G. A. Margulis. Explicit group theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problems of Information Transmission*, 1:51–60, 1988.

[18] M. Morgenstern. Existence and explicit constructions of $q + 1$-regular Ramanujan graphs for every prime power q. *J. Combin. Theory*, B, 62(1):44–62, 1994.

[19] P. Sarnak. *Some applications of modular forms*. Cambridge U. Press, Cambridge, 1990.

[20] M. Sipser and D. A. Spielman. Expander codes. In *Proceedings of the* 35*th IEEE Symposium on Foundations of Computer Science*, 1994.