ASYMPTOTICALLY GOOD FAMILIES

by

Farshid Hajir

Abstract. — We define the general concept of asymptotically good families, and describe them in the context of curves and codes over finite fields, number fields, and regular graphs.

Résumé. — Nous définissons le concept de familles asymptotiquement exactes et décrivons celui-ci pour les courbes et les codes sur les corps finis, les corps de nombres et les graphes réguliers.

1. Introduction

There is a class of optimization problems in various branches of mathematics, including number theory, algebraic geometry, coding theory, and graph theory, that can be classified under one rubric, namely that of "asymptotically good families." In this short article, I sketch some common characteristics for several specific problems and describe a general framework for all of them. The larger aim is to encourage and enlarge study of the deep and fruitful analogies that exist between them, and especially to stimulate further cross-fertilization of ideas and methods.

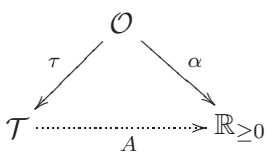
A very well-established analogy of this type is that between number fields and function fields of curves: it has motivated much of the advances in arithmetic and algebraic geometry. Analogies and other types of connections between codes and graphs have proven to be very fruitful to both fields as well. Starting in the 1980s, the construction of codes using methods of algebraic geometry revitalized both coding theory and the study of varieties with extremal properties. Less well-explored are connections between the theory of number fields and those of graphs and codes: it is hoped that studying these connections in the context of asymptotically good families may enrich all these domains of study, for example by bringing to the attention of researchers in any one of these fields methods and ideas which are natural in one or more of the others.

The author was supported by a grant from the NSA.

Especially since it's quickly done, it will be instructive to give, right from the outset, a description of the formalization of the concept of asymptotically good families, prior to discussing the instances which led to the more abstract definition. To begin, we require a *context* $\mathscr{C} = (\mathcal{O}, \mathcal{T}, \tau, \alpha)$, where $\mathcal{O}, \mathcal{T}$ are sets and τ, α are maps $\tau : \mathcal{O} \to \mathcal{T}$ and $\alpha : \mathcal{O} \to \mathbb{R}_{\geq 0}$. Here, $\mathcal{O}$ is the set of objects of interest, $\mathcal{T}$ is a paramater space of *types* of the objects, and α is the *critical invariant* measuring the "quality" of the object. The parameter space is usually a familiar and countable set; for convenience, we will assume that τ is surjective. It goes without saying that our normalization is such that "good" objects are those of high quality.
What interests us in particular is not any single object of high quality (a "gem"), but an infinite necklace on which we may hang a sequence of gems. More precisely, a *family* $\mathcal{F}$ in $\mathcal{O}$ is a sequence $F_1, F_2, \cdots$ of **pairwise distinct** elements of $\mathcal{O}$. We say that $\mathcal{F} = (F_i)$ is *isotypic of type* t if every member of $\mathcal{F}$ has type t, i.e. $\tau(F_i) = t$ for all i. We extend α to families by putting $\alpha(\mathcal{F}) = \liminf_{i\to\infty} \alpha(F_i)$, for $\mathcal{F} = (F_1, F_2, \cdots)$ and say that $\mathcal{F}$ is *asymptotically good* if $\alpha(\mathcal{F}) > 0$. In the contexts we have in mind, it is typically difficult to construct asymptotically good families, or at least to do so explicitly.
With these preliminaries in place, we can now define the main object of interest attached to a context $\mathscr{C} = (\mathcal{O}, \mathcal{T}, \tau, \alpha)$, namely the *asymptotic envelope* function $A : \mathcal{T} \to \mathbb{R}_{\geq 0}$ given by

$$A(t) := \sup_{\mathcal{F} \text{ of type } t} \alpha(\mathcal{F}),$$

where the limit is taken over all isotypic families of type t. Thus, the map A is induces by τ and α as in the following diagram.



It is clear that the asymptotic envelope function is a measure not of the quality of individual objects, but rather of the quality of infinite non-repeating strings of those of a fixed type. We will say that functions $L, U : T \to \mathbb{R}_{\geq 0}$ are lower, respectively, upper bounds for A in the context $\mathscr{C}$ if

$$L(t) \leq A(t) \leq U(t) \text{ for all } t \in T.$$

In most cases we will discuss, we will be able to estimate $A(t)$ by upper and lower bounds but of course would like to have an explicit formula for $A(t)$ itself. Typically, the theory provides a natural and "decent" upper bound, meaning one that is believed to be sharp. Interestingly, the source of this upper bound is usually a zeta function known or at least suspected to satisfy an appropriate Riemann hypothesis. Obtaining lower bounds $L(t)$ involves the creation of examples with extremal properties, usually from objects carrying inordinately many symmetries – it is not surprising that automorphic forms are a typical source. What has been at times a revelation is that automorphic forms are at the root of good lower bounds

even in contexts that do not at first glance appear to be related to number theory or algebraic geometry.

2. Some Examples

Now let us introduce the contexts $\mathscr{C}_{\mathrm{ff}}$ (function fields), $\mathscr{C}_{\mathrm{nf}}$ (number fields), $\mathscr{C}_{\mathrm{lc}}$ (linear codes), and $\mathscr{C}_{\mathrm{rg}}$ (regular graphs), by specifying their types, critical invariants etc. and describing the known lower and upper bounds for their asymptotic envelopes. There are many other contexts that fit the general framework, for example that of tightly packed lattices in Euclidean space, but we will treat them elsewhere. Naturally, the reader is encouraged to be on the lookout for other contexts which fit into the rubric of asymptotically good families!

2.1. Function Fields of Curves over Finite Fields. — To introduce the context $\mathscr{C}_{\mathrm{ff}}$ let $\mathcal{O} = \mathcal{O}_{\mathrm{ff}}$ be the set of all extensions $K/\mathbb{F}(x)$ where $|\mathbb{F}|$ and $[K : \mathbb{F}(x)]$ are both finite. In other words, our objects are function fields of smooth projective geometrically irreducible curves over a finite field, i.e. transcendence degree 1 fields over finite fields, but note that our curves come equipped with a particular map to the projective line. The space of types $\mathcal{T}_{\mathrm{ff}} = Q$ is the set of all prime powers, i.e. of integers $q = p^m$ where p is a prime and m is a positive integer, and $\tau(K/\mathbb{F}(x)) = \tau_{\mathrm{ff}}(K/\mathbb{F}(x)) := |\mathbb{F}|$. Last but not least, we define the critical invariant α by

$$\alpha(K/\mathbb{F}_q(x)) = \alpha_{\mathrm{ff}}(K/\mathbb{F}_q(x)) := \frac{|N_1(K/\mathbb{F}_q)|}{g(K)},$$

where $g(K)$ is the genus of K (or of the curve X corresponding to K) and $N_1(K/\mathbb{F}_q) = |X(\mathbb{F}_q)|$ is the number of degree 1 primes of $K_{/\mathbb{F}_q}$, or, what is the same, the number of $\mathbb{F}_q$-rational points of X. Roughly speaking, the idea is to find curves with many points, as measured against the genus of the curve. The upper bound for the critical invariant $\alpha(K)$ for an individual K comes from the Hasse-Weil bound:

$$N_1(K/\mathbb{F}_q(x)) \leq q + 1 + 2g(K)\sqrt{q}.$$

It is a reflection of the fact that the zeta function of K satisfies the Riemann Hypothesis. When applied to families, this already gives the bound $A_{\mathrm{ff}}(q) \leq 2\sqrt{q}$. Taking this much further, Serre, Ihara and Drinfeld-Vladut obtained a succession of improvements yielding, for an asymptotically good family of curves of fixed type q, $U_{\mathrm{ff}}(q) = \sqrt{q} - 1$. Via a class-field tower construction involving a graph argument, Serre (see **[S]** and **[EHKPWZ]**) gave a general lower bound for $A_{\mathrm{ff}}(q)$: $L_{\mathrm{ff}}(q) = C \log(q)$ for a positive absolute constant C. When m is even, and $q = p^m \geq 49$, a *much* better lower bound is obtained by using modular curves, actually reaching the Drinfeld-Valdut upper bound, thus proving that $A(p^{2k}) = p^k - 1$ if $p^k \geq 7$.

2.2. Number Fields. — For the context of number fields $\mathscr{C}_{\mathrm{nf}}$, the set of objects $\mathcal{O}_{\mathrm{nf}}$ consists of fields K of finite degree $n(K)$ over $\mathbb{Q}$. The type of a number field is defined to be $\tau(K) = r_1(K)/n(K)$; it is the proportion of the embeddings of K into $\mathbb{C}$ with image contained in $\mathbb{R}$.

The space of possible types in this context is $\mathcal{T} = [0,1] \cap \mathbb{Q}$. As the critical invariant, we choose the *recriprocal logarithmic root discriminant*:

$$\alpha_{\mathrm{nf}}(K) := \frac{n(K)}{\log|\mathrm{disc}(K)|},$$

where $\mathrm{disc}(K)$ is the absolute discriminant of K and $n(K) = [K : \mathbb{Q}]$ is its absolute degree; for the field $\mathbb{Q}$, we put $\alpha(\mathbb{Q}) = 0$. Under the Generalized Riemann Hypothesis (GRH), we have a bound due to Stark, Odlyzko and Serre, namely

$$A_{\mathrm{nf}}(t) \leq U^*(t) := (\log(8\pi) + \gamma + \pi t/2)^{-1}.$$

The "*" is to remind us that this holds under the additional assumption of GRH. There is an unconditional upper bound as well; see **[Od]** for more details on these bounds. As for lower bounds, the only source of good families in $\mathscr{C}_{\mathrm{nf}}$ we currently know are nested fields $K_0 \subsetneq K_1 \subsetneq \cdots$ which are ramified at finitely many places and shallowly ramified (they exist by a theorem of Golod and Shafarevich). As a result we do not have an explicit lower bound $L(t)$, though by **[HM]**, we have $A(0) \geq 1/\log(83)$ and $A(1) \geq 1/\log(955)$. Most researchers believe the upper bound $U^*(t)$ is sharp. Note that $U^*(0) \approx 1/\log(44.7)$ and $U^*(1) \approx 1/\log(215.3)$.

2.3. Linear Codes. — Now consider the context $\mathscr{C}_{\mathrm{lc}},$, with $\mathcal{O}_{\mathrm{lc}}$ being the set of all linear codes over finite fields; a general reference is **[TV]**. Recall that a linear code of *length* n and *dimension* k over $\mathbb{F}_q$ is a k-dimensional linear subspace of $\mathbb{F}_q^n$. As in the case of $\mathscr{C}_{\mathrm{ff}}$, we define the type of a linear code $C/\mathbb{F}_q$ to be $q = p^m$. We equip $\mathbb{F}_q^n$ with the Hamming metric,[(1)] and let d be the minimum distance between two distinct codewords (elements of C). A code can be used for communicating through a noisy channel in a way that allows for the correction of errors that may occur through transmission, at the cost of transmitting at a lower efficiency rate. We define the *quality* of a linear code C of dimension k, length n and minimum distance d to be $\alpha(C) = kd/n^2$. The ratios $R(C) = k/n$ and $\delta(C) = d/n$ are known as the *rate* and *relative distance* of C; they both belong to the unit interval. The closer the rate is to 1, the more efficient the code is, while the closer the relative distance is to 1, the greater its capacity for error detection and correction. Since the quality of a code is the product of its rate and its relative distance, a family of codes over $\mathbb{F}_q$ is asymptotically good if and only if the rates and relative distances of its members stay bounded away from 0: this ensures that the codes are efficient and carry good error-correction capabilities. Thanks to the multiplicity of ways for deforming one code into another one with slightly different parameters, we have a "higher resolution" picture of the distribution of asymptotically good families in this context. Namely, consider the set X consisting of limit points of the set of all $(\delta(C), R(C)) \in [0,1]^2$ as C runs over all linear codes over $\mathbb{F}_q$. Then there is a function $\rho_q(\delta)$ such that for all $(\delta_0, R_0) \in [0,1]^2$, (δ_0, R_0) belongs to X if and only if $R_0 \leq \rho_q(\delta_0)$. We have explicit upper and lower bounds

$$\rho_q^{GV}(\delta) \leq \rho_q(\delta) \leq \rho_q^{JPL}(\delta),$$

(1) the Hamming distance between two vectors is the number of positions in which they differ

which we will not specify here, see [**TV**]. The lower bound is known as the Gilbert-Varshamov bound, and the upper one as the JPL Bound (its authors worked at the Jet Propulsion Laboratory). From these explicit functions, one can extract explicit lower and upper bounds $L_{\mathrm{lc}}(q)$ and $U_{\mathrm{lc}}(q)$ for $A_{\mathrm{lc}}(q)$.

2.4. Regular Graphs. — Our last context $\mathscr{C}_{\mathrm{rg}}$ has as its objects $\mathcal{O}_{\mathrm{rg}}$, the set of connected finite regular graphs; a general introduction is given in the survey article [**HLW**], to which we refer for the results discussed below. Recall that a t-regular graph is a graph whose vertices all have degree t, i.e. have t edges emanating from them. We define the type of a graph $G = (V, E) \in \mathcal{O}_{\mathrm{rg}}$ to be the degree t of any one of its vertices $v \in V$ and suppose $t \geq 3$, thus $\mathcal{T}_{\mathrm{rg}} = \mathbb{Z}_{\geq 3}$. Self-loops and multiple edges are allowed for our graphs. If $S \subseteq V$, we let ∂S be the set of edges from S to its complement $V \setminus S$. We will discuss two types of critical invariants for t-regular graphs. First, we may work with $\alpha^{\mathrm{er}}(G) = h(G)$ where $h(G)$ is the *edge expansion ratio* of G, defined by

$$h(G) = \min_{S \subseteq V, |S| \leq |V|/2} \frac{|\partial S|}{|S|}.$$

Alternatively, the adjacency matrix of G (with rows and columns indexed by V having u, v-entry equal to the number of edges from u to v) is a real symmetric n by n matrix. Writing its eigenvalues as $t = \lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_n \geq -t$, we let $\lambda(G) = \lambda_1(G)$ be its "second" eigenvalue. Let us define the "spectral gap" of a t-regular graph G to be $\alpha^{\mathrm{sg}}(G) = t - \lambda(G)$. This quantity is closely related to $h(G)$ via the Dodziuk/Alon-Milman theorem:

$$\frac{t - \lambda(G)}{2} \leq h(G) \leq \sqrt{2t}\sqrt{t - \lambda(G)}.$$

Consequently, a family of t-regular graphs is asymptotically good with respect to the critical invariant α^{er} if and only if it is good with respect to α^{sg}. Such a family is called a family of *expander graphs.* They have many applications in cryptography as well as coding theory, not to mention other branches of mathematics. Let us work with α^{sg}, the spectral gap from now on. By a theorem of Alon-Boppana, we have the upper bound

$$A^{\mathrm{sg}}(t) \leq t - 2\sqrt{t-1},$$

i.e. we can take $U^{\mathrm{sg}}(t) = t - 2\sqrt{t-1}$. As in the previous cases, to obtain a lower bound, we must construct families of t-regular graphs of large spectral gap.
The best we can hope for is such a family which meets the upper bound $t - 2\sqrt{t-1}$. With this in mind, we say that a graph is *t-Ramanujan* if it is t-regular and satisfies $\alpha^{\mathrm{sg}}(G) \geq t - 2\sqrt{t-1}$. (Usually this is stated in the equivalent formulation: $\lambda(G) \leq 2\sqrt{t-1}$). Thus, if $t \geq 3$ is an integer such that a family of t-Ramanujan graphs exist, then $A^{\mathrm{sg}}(t) = t - 2\sqrt{t-1}$. Thanks to the work of Lubotzky, Phillips, Sarnak, Margulis, Morgenstern ..., it is known that if $t - 1$ is a prime power, then families of t-Ramanujan graphs exist. The known constructions are all "automorphic" at root. We also note that a regular graph is t-Ramanujan if and only if its Ihara zeta function satisfies the Riemann Hypothesis (Cor. 4.5.9 of Lubotzky [**L**]).

3. Some Open Questions

The analogies sketched above go quite a bit deeper in certain situations. Namely, for some of the ordered pairs of contexts introduced above, there are known constructions which map an asymptotically good family $\mathcal{F} = (F_1, F_2, \ldots)$ of objects in $\mathscr{C}$ to an asymptotically good family $\mathcal{F}'$ in $\mathscr{C}'$, together with an estimate for $\alpha(\mathcal{F}')$ in terms of $\alpha(\mathcal{F})$.

For example, if $\mathscr{C} = \mathscr{C}_{\mathrm{ff}}$ and $\mathscr{C}' = \mathscr{C}_{\mathrm{lc}}$, then the Goppa construction of algebraic-geometric codes gave a totally unexpected improvement on the Gilbert-Varshamov lower bound (for $q \geq 49$). It also led indirectly to the determination of $A_{\mathrm{ff}}(p^m)$ for all even m. By contrast, the mapping of certain types of good families from $\mathscr{C}_{\mathrm{nf}}$ to $\mathscr{C}_{\mathrm{lc}}$ by Guruswami [**Gu**] is not very well-studied. Another highly important such mapping is from expander graphs to linear codes, giving the first construction of asymptotically good codes that can be coded and decoded in linear time.

It's clear that among the four contexts introduced here, the one about which we know the least is number fields. It would be highly interesting to find an "automorphic" construction of asymptotically good families of number fields, or a method for producing them from an asmptoticaly good family of codes or graphs. Currently, the only known method in the number field context is the Golod-Shafarevich criterion. Is it possible to adapt the probablistic methods that have proved so fruitful in other contexts to this setting?

Note also that for number fields, we do not yet have an explicit lower bound $L_{\mathrm{nf}}(t) \leq A_{\mathrm{nf}}(t)$. It's reasonable to expect a bound $L_{\mathrm{nf}}(t) = ((t-1)\log(83) + t\log(955))^{-1}$, i.e. to fit a "convex" function to the two boundary points that we have. However, this seems to be quite out of reach at the moment, because it involves problems of signatures of units which are quite mysterious.

The major open problem in the context of regular graphs is clearly: For which $t \geq 3$ do families of t-Ramanujan graphs exist? Hoory, Linial and Wigderson conjecture that families of t-Ramanujan graphs exist for all $t \geq 3$ (Conjecture 5.13 of [**HLW**]). Thus, they conjecture that

$$A^{\mathrm{sg}}(t) =^{?} t - 2\sqrt{t-1} \text{ for all } t \geq 3.$$

The best evidence for this conjecture is probably the theorem of Friedman to the effect that for any $\epsilon > 0$, fixed t and n tending to infinity, the probability that a random t-regular graph on n vertices has $\lambda(G) \leq 2\sqrt{t-1} + \epsilon$ is $1 - o_n(1)$.

Both in the case of $\mathscr{C}_{\mathrm{ff}}$ and $\mathscr{C}_{\mathrm{rg}}$, since we know that the upper bound is sharp for a substantial subset of parameters $t \in \mathcal{T}$, it is tempting to believe that it is so for all values of t. There is a simple, but deep, example in which that turns out not to be the case: namely for the Shannon capacity of cyclic graphs. To define the context $\mathscr{C}_{\mathrm{sc}}$, let $\mathcal{O}_{\mathrm{sc}} = \{C_t^n | n \geq 1, t \geq 3\}$ be the set of all n-fold self-products of the cyclic graph C_t on t vertices (say a regular t-gon). As in the case of regular graphs, we have $\mathcal{T} = \mathcal{T}_{\mathrm{sc}} = \mathbb{Z}_{\geq 3}$ and $\tau(C_t^n) = t$. To introduce the critical invariant, recall that For a graph G, the independence number of G, $\mathrm{int}(G)$, is the size of a maximal subset of its vertices not joined by any edges. The critical invariant, the

Shannon capacity, is defined by

$$\alpha_{\mathrm{sc}}(C_t^n) := \frac{\log_2(\mathrm{int}(C_t^n))}{n}.$$

We refer the reader to [**AZ**] for the information-theoretic motivation of this definition. Shannon showed that $A_{\mathrm{sc}}(t) \leq t/2$ for all t. It is then very easy to show that for even integers t, $A_{\mathrm{sc}}(t) = t/2$ but Shannon discovered that the computation of $A_{\mathrm{sc}}(t)$ for odd $t \geq 5$ is highly non-trivial, and he was unable to determine even $A(5)$. Note that as in the case of $\mathscr{C}_{\mathrm{ff}}$, there is a simple formula for $A_{\mathrm{sc}}(t)$ for exactly half of the types, and one could guess that $A_{\mathrm{sc}}(t) = t/2$ for all $t \geq 3$. However, it turns out that for odd $t \geq 5$,

$$(t-1)/2 < A_{\mathrm{sc}}(t) \leq \frac{t}{1 + (\cos(\pi/t))^{-1}} < t/2.$$

It is known by a celebrated theorem of Lovasz that the middle inequality above is sharp for $t = 5$, but the value of $A_{\mathrm{sc}}(t)$ is not known for larger odd t; see [**AZ**] for more details.
Just as the existence of t-Ramanujan graphs for $t \neq p^e + 1$ is unknown, leaving the possibility that for such t there is a strict inequality $A_{\mathrm{rg}}(t) < U_{\mathrm{rg}}(t) = t - 2\sqrt{t-1}$, for $q = p^m$ with m odd, we have

$$C \log(p^m) \leq A_{\mathrm{ff}}(p^m) \leq \sqrt{p^m} - 1,$$

with the upper bound sharp for even m but not known to be so for odd m. It would be of great interest to find a single prime p for which we can determine whether $A_{\mathrm{ff}}(p) = \sqrt{p} - 1$ is true or false.

References

[AZ] Aigner, Martin; Ziegler Gunter M. Proofs from The Book. Including illustrations by Karl H. Hofmann. Third edition. Springer-Verlag, Berlin, 2004. viii+239 pp.

[EHKPWZ] Elkies, Noam D.; Howe, Everett W.; Kresch, Andrew; Poonen, Bjorn; Wetherell, Joseph L.; Zieve, Michael E. Curves of every genus with many points. II. Asymptotically good families. Duke Math. J. 122 (2004), no. 2, 399–422.

[Gu] Guruswami, Venkatesan Constructions of codes from number fields. *IEEE Trans. Inform. Theory* **49** (2003), no. 3, 594–603.

[HM] Hajir, F.; Maire, C. Tamely ramified towers and discriminant bounds for number fields II, *J. Symb. Comp.* 33 (2002), no. 4, 415–423.

[HLW] Hoory, Shlomo; Linial, Nathan; Wigderson, Avi Expander graphs and their applications *Bull. Amer. Math. Soc.* **43** (2006), 439-561.

[L] Lubotzky, Alexander Discrete groups, expanding graphs and invariant measures. With an appendix by Jonathan D. Rogawski. Progress in Mathematics, 125. Birkhauser Verlag, Basel, 1994. xii+195 pp.

[Od] Odlyzko; A.M. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results, *Sém. de Théorie des Nombres, Bordeaux* **2** (1990), 119-141.

[S] Serre, J.P. Rational points on curves over finite fields, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.

[TV] Tsfasman, M. A.; Vladut, S. G. Algebraic-geometric codes. Translated from the Russian by the authors. Mathematics and its Applications (Soviet Series), 58. Kluwer Academic Publishers Group, Dordrecht, 1991. xxiv+667 pp.

May 3, 2010

Farshid Hajir, Department of Mathematics and Statistics, University of Massachusetts, Amherst MA 01003, USA. • *E-mail :* hajir@math.umass.edu