Arithmetic Groups, Ramanujan Graphs and Error Correcting Codes

Alex Lubotzky
Einstein Institute of Mathematics, Hebrew University
Jerusalem 91904, ISRAEL

joint with Tali Kaufman

§1. Codes

An **(n, k, d)-code** is a subspace of $\mathbb{F}_2^X$ with
$|X| = n =$ the length of the code
of dimension $k =$ the dimension of the code
and distance $d = \min\{wt(v) | 0 \neq v \in C\}$
where Hamming weight $wt(v) = \#$ non-zero bits.

Denote
- $r(c) = \frac{k}{n} =$ rate
- $\delta(c) = \frac{d}{n} =$ normalized distance

Good Codes $n \to \infty, \quad r(c), \delta(c) \geq \varepsilon > 0.$

For a code C denote

$$C^{\perp} = \{w \in \mathbb{F}_2^X | w \cdot v = 0 \quad \forall v \in C\}$$

where $w \cdot v$ - the usual inner product $\sum_{i=1}^{n} w_i v_i$.

The dual code $C^{\perp}$ can be thought as the space of constraints (linear functionals on $\mathbb{F}_2^x$) defining C (as $C = (C^{\perp})^{\perp}$).

The code C (when $n \to \infty$) is called LDPC (low density parity check) if there exists a set of defining constraints of bounded weight.

- C is **symmetric** if $\exists$ a group H acting transitively on X (and so on $\mathbb{F}_2^X$) preserving C.
  - All variables look alike

- C is **single-orbit symmetric** if $\exists w \in C^\perp$ s.t. $H.w$ spans $C^\perp$.
  - All constraints are "the same"

- C is **highly symmetric** if this w is of bounded weight

$$(\Rightarrow LDPC)$$

Basic question (Kaufman, Sudan, Wigderson)

To what extent can symmetric LDPC codes attain (or even come close to) the coding theory gold standards of linear distance and constant rate?

Many/Most codes studied classically are cyclic codes:

Def. $C \leq \mathbb{F}_2^n$ is cyclic if

$$(a_0, \ldots, a_{n-1}) \in C \Leftrightarrow (a_{n-1}, a_0, \ldots, a_{n-2}) \in C$$

i.e. symmetric under the cyclic group.

But, a long standing:

Conj: *There are no cyclic good codes.*

Some partial results:
Berman (1967): True, if the prime factors of n are bounded

Babai-Shpilka-Stefankovic: There are no cyclic LDPC good codes.

Kaufman-Wigderson extended this to solvable groups (of bounded derived length) and also prove some results of having codes not so far from good. But were skeptical about existence of good symmetric LDPC.

Main Thm (Kaufman-Lubotzky)

There exist highly symmetric LDPC good codes.

so:
- *constant rate*
- *constant relative distance*
- *symmetric under a group action H*
- *the dual $C^{\perp}$ is generated by a single H-orbit $H \cdot w$.*
- *w can be chosen to have bounded weight*
- *C is LDPC*

§2. Cayley Codes

G a group, $|G| = m$
$S \subseteq G, \quad S = S^{-1}, \quad G = \langle S \rangle$.
$Cay(G; S)$ - the Cayley graph $g \sim gs, \;\; g \in G, s \in S$

$$E = \text{edges}, \quad |E| = \frac{m|S|}{2}$$

Let $B \subseteq \mathbb{F}_2^S$ a code ("small code")

Define

$$C(G, S, B) = \{f \in \mathbb{F}_2^E | \forall g \in G, f_g \in B\}$$

f_g is the "local view" of f in g - i.e. $f_g(s) := f(g \leftrightarrow gs)$.

Thm (Sipser-Spielman; inspired by Tanner)

$C = C(G, S, B)$ is a linear code with $n = \frac{|G|\,|S|}{2}$ and

- $r(C) \geq 2r(B) - 1$
- $\delta(C) \geq \left(\frac{\delta(B)-\lambda}{1-\lambda}\right)^2$

when $\lambda =$ second normalized eigenvalue of $Cay(G, S)$

$$\text{e.v.}'s \text{ are } \lambda_0 = |S| > \lambda_1 \geq \ldots \geq \lambda_{|G|-1}, \qquad \text{so } \lambda = \frac{\lambda_1}{|S|}$$

Cor

If $r(B) > \frac{1}{2}$ and $\delta(B) > \lambda$, we get good LDPC codes (not yet symmetric! but LDPC if $|G| \to \infty$ with $|S|$ bounded).

Idea of Proof

(A) rate: compute number of equations

(B) **Alon-Chung Lemma** X r-regular graph with $\lambda(X) = \lambda$.
If $Y \subseteq X$ of size $\gamma|X|$ $(0 < \gamma < 1)$ then
$|E(Y)| \leq \frac{r|X|}{2}(\gamma^2 + \lambda\gamma(\gamma - 1))$ i.e., the expected number $\gamma^2 \frac{r|X|}{2}$ (as for random) plus an error term bounded using λ.

Now if $f \in C(G, S, B)$ with some support, by the Lemma cannot concentrate on **too** small set of vertices, hence the average number of edges per vertex is smaller than $\delta(B)$ - a contradiction.

How to make it symmetric?

Assume a group T acting on G, i.e., $\rho : T \to Aut(G)$ an homo and $\exists s \in S$ with: $S = \{\rho(t)(s) | t \in T\}$ i.e. S is one orbit of T.

Let $H = G \rtimes T$ semi-direct product

$$G \rtimes T = \{(g, t) \in G \times T\} \quad (g_1, t_1) \cdot (g_2, t_2) = (g_1 \cdot \rho(t_1)g_2, t_1 t_2)$$

Prop: [Kaufman–Wigderson]

1. H acts on $Cay(G, S)$ as an edge transitive automorphism group.
2. If B is symmetric (resp: and single orbit) under S, then so is C.

§3. Edge transitive Ramanujan graphs

An r-regular finite connected graph X with adjacency matrix $A = A_x$ is called **Ramanujan** if for every eigenvalue μ of A, either $|\mu| = r$ or $|\mu| \leq 2\sqrt{r-1}$.
So: for such X, $\lambda(X) \leq \frac{2\sqrt{r-1}}{r}$

r-regular Ramanujan graphs for $r = p + 1$ (p prime)
(Lubotzky-Phillips-Sarnak/Margulis, 80's)
and for $r = q + 1, q$ prime-power (Morgenstern, 90's).

But these are (probably) **not** edge transitive. But:

Thm (Lubotzky-Samuels-Vishne - 2005)

$\forall\, q$ prime power and $\alpha \in \mathbb{N}$, with $q^\alpha > 17$, let $G = PSL_2(q^\alpha)$ or $G = PGL_2(q^\alpha)$ and T the non-split tori of order $q+1$ in $PGL_2(q)$. Then $\exists \tau \in G$ such that $Cay(G, S)$ is $(q+1)$-Ramanujan with $S = \{t\tau t^{-1} | t \in T\}$.

Non-split tori means:
$\mathbb{F}_{q^2}^* = \mathbb{F}_{q^2} \setminus \{0\}$ acts on $K = \mathbb{F}_{q^2}$ by multiplication.
K is a 2-dim vector space over $\mathbb{F}_q$ and the action is $\mathbb{F}_q$-linear.
This gives a homo:
$\mathbb{F}_{q^2}^* \to GL_2(\mathbb{F}_q)$, the image contains the center of order $q-1$, so when projected to $PGL_2(\mathbb{F}_q)$ we get a group of order $\frac{q^2-1}{q-1} = q+1$ - the **non-split tori** T.
Note: T acts transitively on the projective line $P^1(\mathbb{F}_q)$.

- The big picture
- Ramanujan complexes
- The Cartwright-Steger lattices.

§4. Cyclic codes of prescribed parameter

We want to use $G = PSL_2(q^\alpha)$ or $PGL_2(q^\alpha)$ as above, so $\lambda \leq \frac{2\sqrt{q}}{q+1}$.
We now need a "small code" on $\mathbb{F}_2^{q+1}$: T is a cyclic group so we need a cyclic code B on $\mathbb{F}_2^{q+1}$ with

$$r(B) > \tfrac{1}{2} \text{ and } \delta(B) > \frac{2\sqrt{q}}{q+1}$$

.

Fortunately, we need it only for one q!!!

Quick Review on Cyclic Codes

$$V \approxeq \mathbb{F}_2^n \simeq \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \,\big|\, a_i \in \mathbb{F}_2\}$$
$$\simeq \mathbb{F}_2[x]/(x^n - 1) =: R$$

Cyclic Code B is an ideal of R generated by a polynomial $h(X)$ with $h(X)|X^n - 1$. In this case $\dim B = n - \deg h(x)$. But is much more difficult to estimate distance (or δ) of B (recall the long standing problem on good cyclic codes).

Best understood are the $BCH(r, m)$ codes:
$n = 2^m - 1, \qquad E = \mathbb{F}_{2^m}, \quad w$ a primitive element of order n.
For $\alpha \in E$, let

$$m_\alpha(x) = \text{min poly of } \alpha,$$

$$h_r(x) = l.c.m.\{m_{w^i}(x) | i = 1, \ldots, r\}$$

and $B = BCH(r, m)$ the ideal generated by $h_r(x)$.

Prop:

$$\dim(B) \geq n - \frac{mr}{2}, \qquad \text{distance } (B) \geq r + 1$$

This could be OK but $2^m - 1 \neq q + 1$ to any prime power! Even worse all BCH codes over $\mathbb{F}_2$ are of odd length! We need even!

Lemma (based on van Lint)
If $\exists$ a binary cyclic code B of (odd) length $n = 2^m - 1$, dimension k and distance d, then there exists an (explicit) binary code of length $2n$, dimension $2k$ and distance d.

Now, we only need to look for $2(2^m - 1) = q + 1$ i.e.
$q = 2^{m+1} - 3$ is a prime (power).

Are there infinitely many such? We do not know (recall Mersenne primes $2^{m+1} - 1$?).

But we need just **one** (plus the inequalities ...)
$2^{12} - 3 = 4093$ is a prime satisfying all conditions!!! $\square$