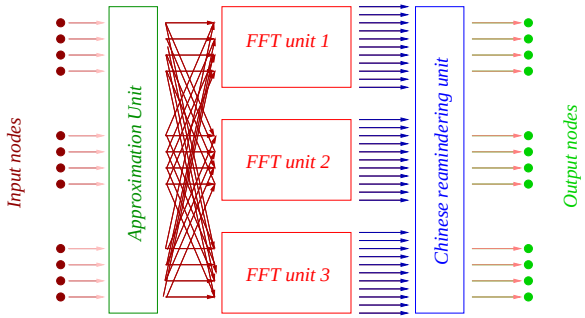
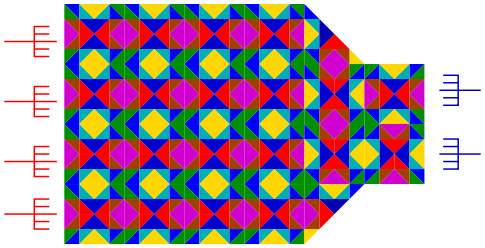
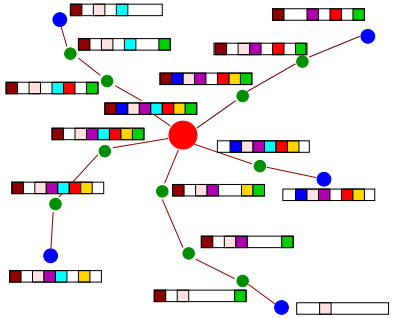
Unusual Applications of Algebra and Discrete Mathematics







Amin Shokrollahi

digitalfountain

Outline

- Precise Fast Fourier Transforms via cyclotomic fields
  (Buhler, Stemann)

- Group representation theory and multiple antenna transmission
  (Hassibi, Hochwald, Sweldens)

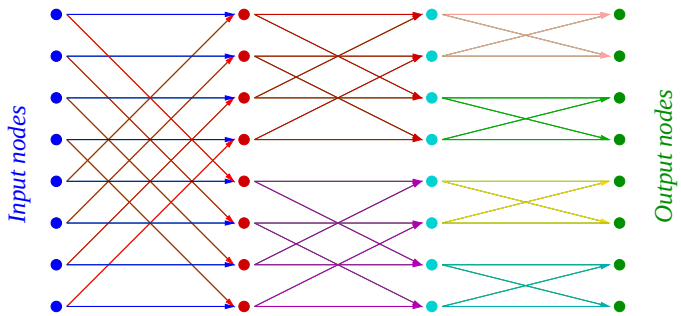
- Delivering content over computer networks
  (Luby, Mitzenmacher, Spielman, Stemann)

Precise Fast Fourier Transforms

Let $N := 2^n$ and $\zeta := e^{2\pi i/N}$. The Discrete Fourier Transform of a complex vector $(a_0, \ldots, a_{N-1})$ is the vector $(\hat{a}_0, \ldots, \hat{a}_{N-1})$ defined by

$$\forall\, j = 0, \ldots, N-1: \quad \hat{a}_j = \sum_{k=0}^{N-1} a_k \zeta^{jk}.$$

Straight-forward computation needs $O(N^2)$ arithmetic operations. Can be done in $O(N \log(N))$ operations. (FFT.)



Precision

At each level of the FFT the inevitable scaling leads to the loss of 1/2 bits on average when working on a fixed point basis.

An FFT- accompanied by an inverse FFT of a vector of length 1024 leads to a loss of 10 bits. This can be fatal on a 16-bit fixed point processor.

Multiple precision fixed point computation yields b-bit accurate FFT's in time

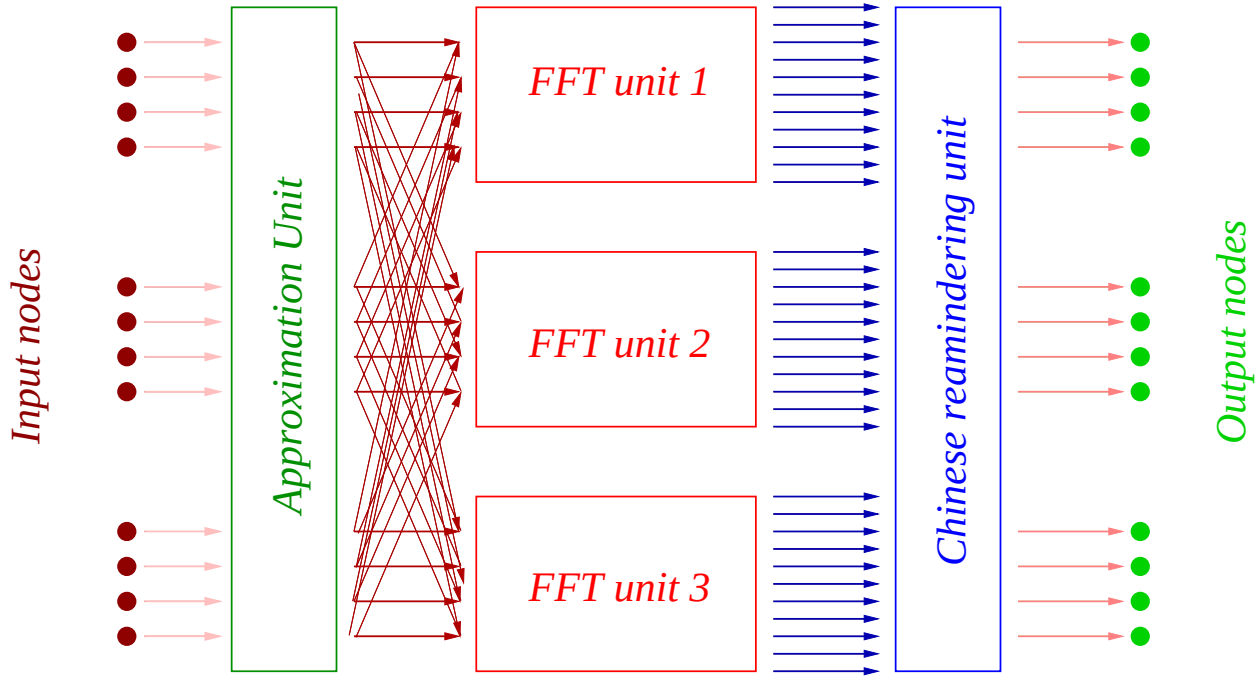
$$O(b^2 N \log(N)).$$

New algorithm does that in time

$$O(b \log(b) N \log(N)).$$

Fixed point FFT processor chart

The following algorithm was proposed by Cozzens and Finkelstein:



Main focus: Approximation unit.

Approximation Problem

For $\zeta := e^{2\pi i/2^n}$ let $\mathbb{Z}[\zeta]_M$ be the set of integral linear combinations of powers of ζ with coefficients bounded by M in absolute value.

Design an algorithm that approximates a given complex number inside the unit circle by an element of the set $\mathbb{Z}[\zeta]_M$.

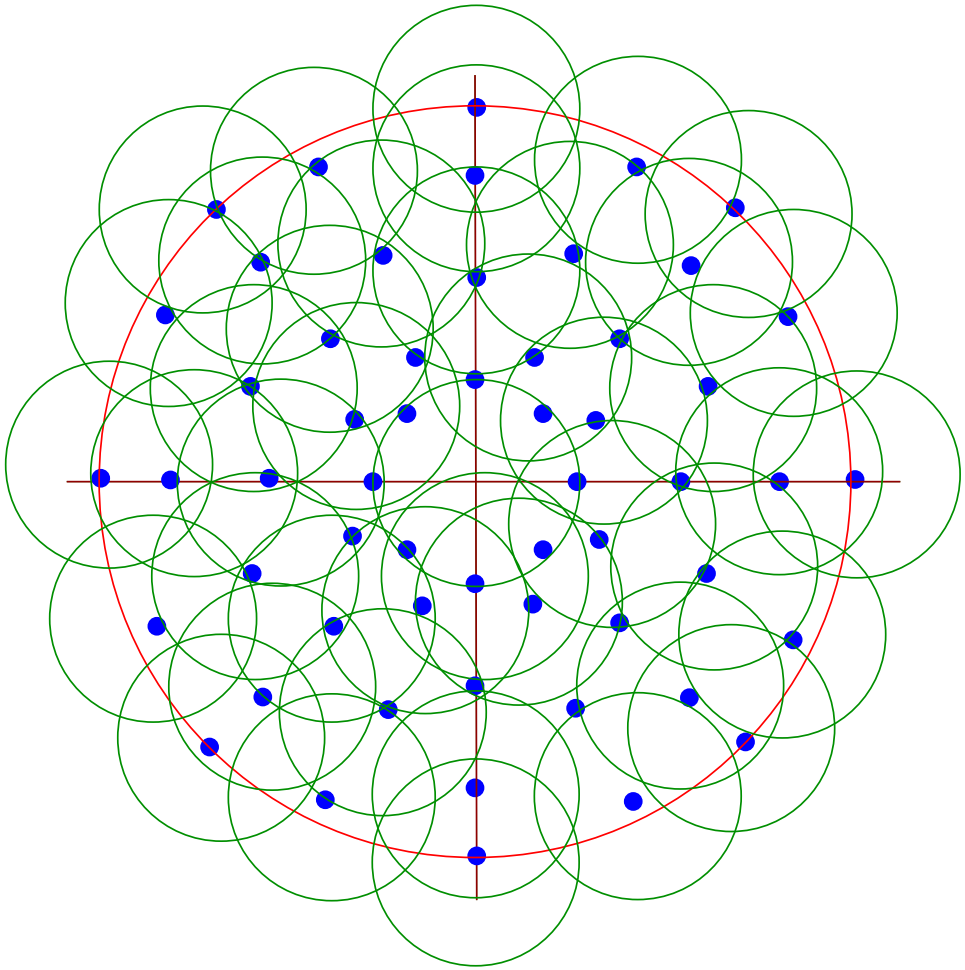
- Cozzens and Finkelstein: general algorithm, optimal error, infeasible since exhaustive search.

- Games: special case $n = 3$, optimal approximation error $\sim 1/M$, running time $O(M)$, however: complicated search structures, not suited for real time applications.

Our algorithm: general, close to optimal error, suited for real time applications.

What can we Expect?

For fixed n any approximation algorithm has a worst case error of $\Omega(1/M^{2^{n-2}-1})$.



Runnig Time and Approximation Error

Suffices to approximate real numbers in maximal real subfield of $\mathbb{Q}(\zeta)$.

Example: $n = 3$: approximation error $\sim 1/M$, running time $O(\log(M))$.

General n: approximation error $\sim 1/M^{2^{n-2}-1}$, running time $O(\log(M))$.

Practical setting: $n = 4$, approximation error $\sim 1/M^3$, running time $O(\log(M))$.

In all these cases the approximation error has optimal order of magnitude.

The exponent $2^{n-2} - 1$ is the Dirichlet number (number of fundamental units) of the cyclotomic field $\mathbb{Q}(\zeta)$.

A Simple Algorithm

Given a real number α between 0 and 1 and an integer M, approximate α by $a + b\sqrt{2}$ for integers a and b such that $|a|, |b| \leq M$.

Example: Suppose we want to approximate 0.1, with $M = 64$.

Let $E := \{-41 + 29\sqrt{2}, 17 - 12\sqrt{2}\} =: \{\varepsilon_1, \varepsilon_2\}$.

Start with the approximation $a_1 := 0$.

Algorithm

$$E := \{-41 + 29\sqrt{2}, 17 - 12\sqrt{2}\} =: \{\varepsilon_1, \varepsilon_2\}.$$

$$a_2 := a_1 + \varepsilon_2 = 17 - 12\sqrt{2} \sim 0.0293$$

$$a_3 := a_2 + \varepsilon_1 = -24 + 17\sqrt{2} \sim 0.0416$$

$$a_4 := a_3 + \varepsilon_2 = -7 + 5\sqrt{2} \sim 0.0711$$

$$a_5 := a_4 + \varepsilon_2 = 10 - 7\sqrt{2} \sim 0.1005$$

$$a_6 := a_5 + \varepsilon_1 = -31 + 22\sqrt{2} \sim 0.1126.$$

Stop with the approximation $a_5 = 10 - 7\sqrt{2}$. The approximation error is 0.005...

Where does E come from?

Continued Fractions

Set E consists of small elements of different signature.

Let $(-1)^\ell(P_\ell - Q_\ell\sqrt{2}) = (-1+\sqrt{2})^\ell > 0$ define the convergents of the continued fraction expansion of $\sqrt{2}$.

$$E := \left\{(-1)^\ell(P_\ell - Q_\ell\sqrt{2}), (-1)^{\ell+1}(P_{\ell+1} - Q_{\ell+1}\sqrt{2})\right\}$$

for suitable ℓ.

The final result is an approximation algorithm with worst case error of $1.71/M$ which compares very well with the lower bound $\Omega(1/M)$.

The algorithm can be modified to run in time $O(\log(M))$.

16th Roots of Unity

Example: Approximation of 0.1 in $\mathbb{Z}[\zeta]_{10}$

Let $\theta_0 := 1$, $\theta_1 := \sqrt{2+\sqrt{2}}$, $\theta_2 := \sqrt{2}$, $\theta_3 := \sqrt{2-\sqrt{2}}$. We use a set E whose elements have the following representation with respect to the above basis:

$$\begin{aligned} E &:= \{(-3,1,3,-4),(6,-3,-3,5),(-5,5,-4,2),\\ &\quad\ (10,-9,7,-4),(-5,-2,4,4),(8,2,-5,-6)\}\\ &=: \{\varepsilon_1,\ldots,\varepsilon_6\}. \end{aligned}$$

We start with $a_1 := 0$:

16th Roots of Unity

$$\begin{aligned} E &:= \{(-3,1,3,-4),(6,-3,-3,5),(-5,5,-4,2),\\ &\quad\ (10,-9,7,-4),(-5,-2,4,4),(8,2,-5,-6)\}\\ &=: \{\varepsilon_1,\ldots,\varepsilon_6\}. \end{aligned}$$

$a_2 := a_1 + \varepsilon_1 = (-3,1,3,-4) \sim 0.0289$

$a_3 := a_2 + \varepsilon_2 = (3,-2,0,1) \sim 0.0698$

$a_4 := a_3 + \varepsilon_1 = (0,-1,3,-3) \sim 0.0988$

$a_5 := a_4 + \varepsilon_3 = (-5,4,-1,1) \sim 1.7422$

We stop with the approximation $a_4 = -\theta_1 + 3\theta_2 - 3\theta_3$.

The error of this approximation is 0.00121....

Galois Spectrum

Let $\zeta = \exp(2\pi i/16)$.

Then $\theta_1 = \zeta + \zeta^{-1}$, $\theta_2 = \zeta^2 + \zeta^{-2} = \sqrt{2}$, and $\theta_3 = \zeta^3 + \zeta^{-3}$.

$\mathbb{Q}(\theta_1)$ is a Galois extension of $\mathbb{Q}$.

Its Galois group is cyclic and is generated by $\tau\colon \zeta + \zeta^{-1} \mapsto \zeta^5 + \zeta^{-5}$.

Galois-Spectrum: Fundamental Equation

For $a = \alpha_0 + \alpha_1\theta_1 + \alpha_2\theta_2 + \alpha_3\theta_3$ we have

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \frac{1}{8} \begin{pmatrix} 2 & 2 & 2 & 2 \\ \theta_1 & -\theta_3 & -\theta_1 & \theta_3 \\ \theta_2 & -\theta_2 & \theta_2 & -\theta_2 \\ \theta_3 & \theta_1 & -\theta_3 & -\theta_1 \end{pmatrix} \begin{pmatrix} a \\ \tau(a) \\ \tau^2(a) \\ \tau^3(a) \end{pmatrix}.$$

$\rightarrow L_\infty(a) \leq \text{maxconj}(a)$

$\rightarrow a$ has signature $(+,-,-,+)$ if $\tau(a)$ is positive and

$$\tau(a) \geq \frac{\theta_1}{\theta_3}(|a| + |\tau^2(a)| + |\tau^3(a)|)$$

$\rightarrow$ similar assertions hold for other signatures.

Cyclotomic Units

Elements of E: power products of small elements with signatures

$$(+,-,-,+),(+,-,+,-),(+,+,-,-).$$

We use cyclotomic units: let

$$\eta_j := \zeta^j \frac{1-\zeta}{1-\zeta^{2j+1}}, \quad j = 1,2,3.$$

η_j is real and is a unit of $\mathbb{Z}[\zeta]$, i.e., the product of its Galois-conjugates is plus or minus one.

This is in complete analogy to the case $n = 3$, since for $\zeta = \mathrm{e}^{2\pi i/8}$ we have $\eta_1 = \sqrt{2} - 1$.

Linear Programming

Find k_1, k_2, k_3 such that $\varepsilon = \prod_{j=1}^{3} \eta_j^{k_j}$ satisfies $|\tau(\varepsilon)| \geq 2\frac{\theta_1}{\theta_3}|\tau^j(\varepsilon)|$ for $j = 2, 3$, and $(1 + \frac{\theta_3}{\theta_1})|\tau(\varepsilon)| \leq 4M - 1$.

Then $L_\infty(\varepsilon) \leq M$ and ε has signature $(+, -, -, +)$ or $(-, +, +, -)$, according to whether $\tau(\varepsilon)$ is positive or not.

Take logarithms:

$$\begin{aligned} \sum_{l=1}^{3} k_l(\log|\tau^j(\eta_l)| - \log|\tau(\eta_l)|) &\leq -\log(2) - \log(\theta_1) + \log(\theta_3) \\ \sum_{l=1}^{3} k_l \log|\tau(\eta_l)| &\leq \log(4M-1) + \log(\theta_1) - \log(\theta_1 + \theta_3). \end{aligned}$$

Minimize $\sum_{l=1}^{3} k_l \log|\eta_l|$ subject to these inequalities. (3 constraints and 3 variables.)

Works because cyclotomic units are indpenedent!

General Algorithm

For $n \geq 5$ there is no signature technique.

However, one can replace the signature by a more complicated attribute based on the magnitude of the Galois-conjugates.

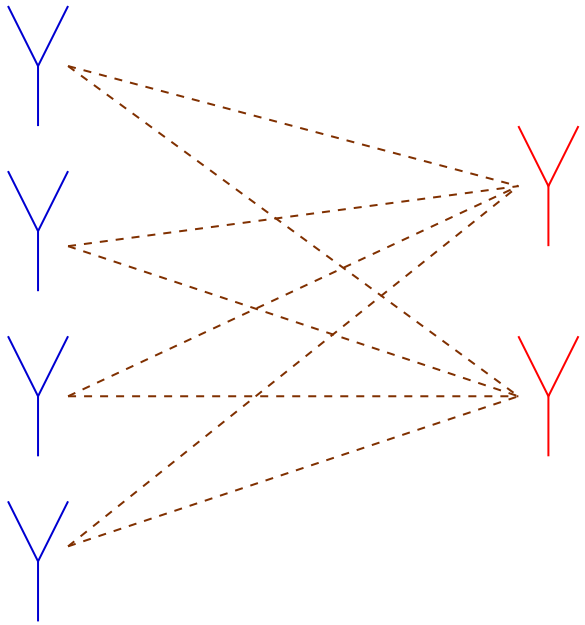
In an analogous way one can construct a set E consisting of power products of cyclotomic units.

The corresponding exponents can be found by solving linear equations of size 2^{n-2}.

The resulting algorithm has optimal worst case error $O(1/M^{2^{n-2}-1})$ for fixed n .

Multiple Antenna Systems

Want to introduce a new packing problem related to the design of modulation schemes for mobile multiple antenna wireless networks and give some solutions using group theory.



Differential Encoding

M transmit antennas.

Codebook consists of L unitary $M \times M$-matrices $\{S_1, S_2, \ldots, S_L\}$ and is called a unitary space-time code.

Signals transmitted:

$$S_{i_1}, S_{i_1} S_{i_2}, S_{i_1} S_{i_2} S_{i_3}, \ldots.$$

Reason: Over a Rayleigh flat fading channel the unknown channel coefficients can be eliminated for decoding.

Probability of Error

Probability of mistaking S and R is lower the larger the diversity distance

$$d(S,R) := \frac{1}{2}|\det(S-R)|^{1/M}$$

is.

Diversity product of $\mathcal{S}$:

$$\zeta(\mathcal{S}) := \min_{S,R\in\mathcal{S},S\neq R} d(S,R).$$

Design problem:
Find a large set $\mathcal{S}$ of unitary $M \times M$-matrices for which $\zeta(\mathcal{S})$ is as large as possible.

Diversity "Distance" and Packing Problems

Diversity distance is **NOT** a metric!

$$d\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) + d\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0$$

but

$$d\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1.$$

Design problem is hard!

Main function:

$$A(M, L) := \sup\{\epsilon \mid \exists \mathcal{S} \subset U(M), \#\mathcal{S} = L, \zeta(\mathcal{S}) \geq \epsilon\}.$$

Upper and lower bounds?

Special Cases

- $A(M,2) = 1$: $\{I_M, -I_M\}$.
- $A(M,3) = \sqrt{3}/2$. (Proof required!)
- $A(1,L) = 2\sin(\pi/L)$.
- $A(2,L) = ?$

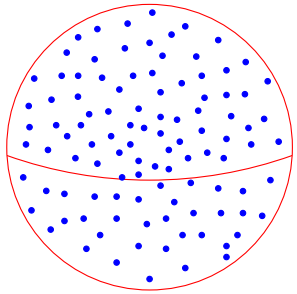
$A(2, L)$

$$SU(2) = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \mid \mathrm{Re}(a)^2 + \mathrm{Im}(a)^2 + \mathrm{Re}(b)^2 + \mathrm{Im}(b)^2 = 1 \right\} \simeq \mathbb{H}^{\times},$$

so nonzero differences in $SU(2)$ are invertible!

$(SU(2), d(\cdot, \cdot))$ is isometric to $\mathbb{S}^3$ with euclidean distance.

Good spherical codes in $\mathbb{R}^4$ yield good differential codes for two transmit antennas



Group Codes

Want to construct finite sets $\mathcal{S}$ of unitary $M \times M$-matrices that form a group under matrix multiplication, and for which

$$\zeta(\mathcal{S}) = \frac{1}{2} \min_{S,R \in \mathcal{S}, S \neq R} |\det(S - R)|^{1/M} \neq 0.$$

Why a group?

- Multiplication of matrices can be done symbolically.
- We have
$$\zeta(\mathcal{S}) = \frac{1}{2} \min_{\mathcal{S} \ni S \neq I} |\det(I - S)|^{1/M}.$$
- Mathematically interesting.

Group Representations

Concentrate on $\zeta(\mathcal{S}) \neq 0$.

No element in $\mathcal{S}$ except for the identity has eigenvalue 1.

Matrix representation: homomorphism of the group into $U(M)$ for some M.

Fixed-point-free (fpf) groups: Groups with a representation Δ such that for $g \in G$ $\Delta(g)$ has eigenvalue 1 iff $g = 1$.

Classification? Done (in large parts) by Zassenhaus in 1936 in the context of near-fields.

Fixed-point-free Abelian Groups

Theorem: An abelian group is fpf iff it is cyclic.

Proof:

- Irreducible representations are characters.
- Character is fpf iff its kernel is trivial.
- Structure theorem for abelian groups: group must be cyclic.

Resulting matrices are diagonal codes (Hochwald and Sweldens'00):

$$\left(\begin{pmatrix} \eta^{u_1} & 0 & \cdots & 0 \\ 0 & \eta^{u_2} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & \eta^{u_M} \end{pmatrix} \right)^k, \quad \eta = \mathrm{e}^{2\pi i/L}, \quad 0 \le k < L.$$

Fixed-point-free p-Groups

Subgroups of fpf-groups are fpf.

Concentrate on p-groups.

Theorem:

- For odd p, a p-group is fpf iff it is cyclic
- For even p, a p-group is fpf iff it is cyclic or a generalized Quaternion group.

Proof: Induction on size of group, and some elementary representation theory.

Classification of fpf groups: Classify all groups all of whose p-Sylow subgroups are of the above form.

Fixed-point-free Groups of Odd Order

All fixed-point-free groups of odd order are of the type

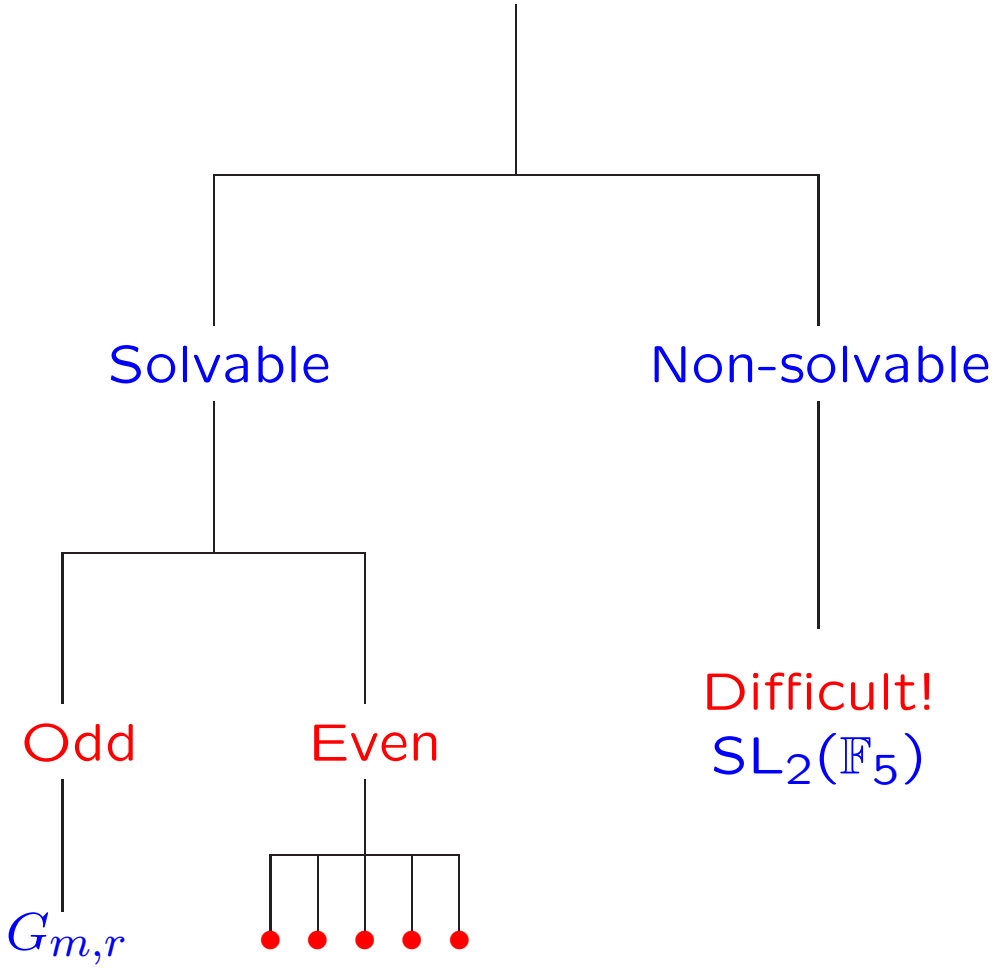
$$G_{m,r} = \langle \sigma, \tau \mid \sigma^m = 1, \tau^n = \sigma^t, \tau^{-1}\sigma\tau = \sigma^r \rangle,$$

where n is the order of $r \bmod m$, $t = m/\gcd(m, r-1)$, and all prime divisors of n divide $\gcd(r-1, m)$.

$G_{21,4}$ gives constellation with 63 signals and $\zeta = 0.3851$.

$$\Delta(\sigma) = \begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^4 & 0 \\ 0 & 0 & \eta^{16} \end{pmatrix}, \quad \Delta(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \eta^7 & 0 & 0 \end{pmatrix}, \qquad \eta = \mathrm{e}^{2\pi i/21}.$$

Structure of Classification

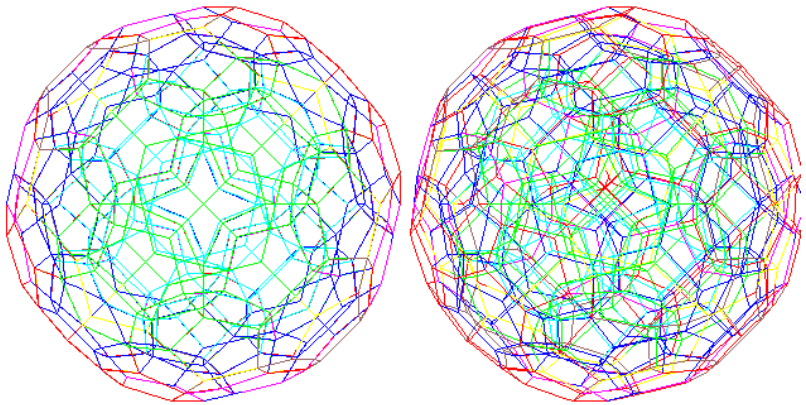


The Group $SL_2(\mathbb{F}_5)$

Both irreducible 2-dimensional representations of this group are fpf.

2-antenna group code of size 120, generated by the matrices

$$P = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta^2 - \eta^3 & \eta - \eta^4 \\ \eta - \eta^4 & \eta^3 - \eta^2 \end{pmatrix}, \quad Q = \frac{1}{\sqrt{5}} \begin{pmatrix} \eta - \eta^2 & \eta^2 - 1 \\ 1 - \eta^3 & \eta^4 - \eta^3 \end{pmatrix}, \qquad \eta = \mathrm{e}^{2\pi i/5}.$$

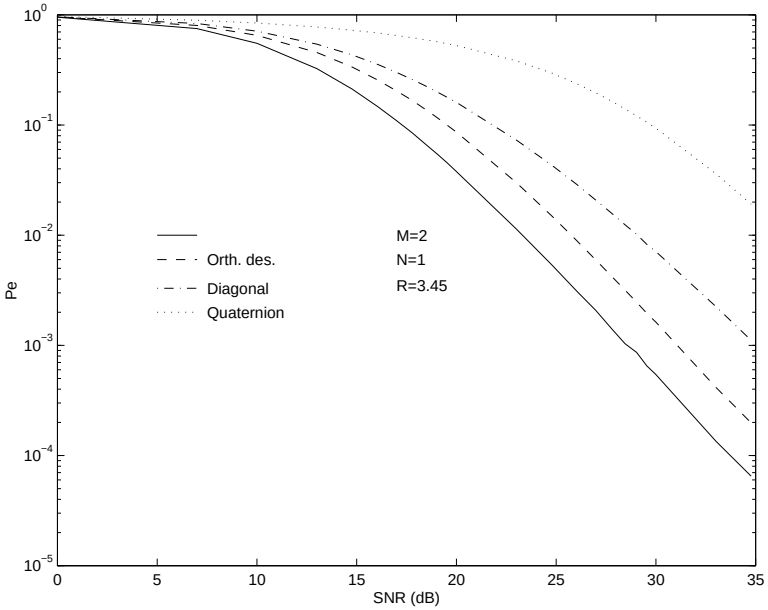


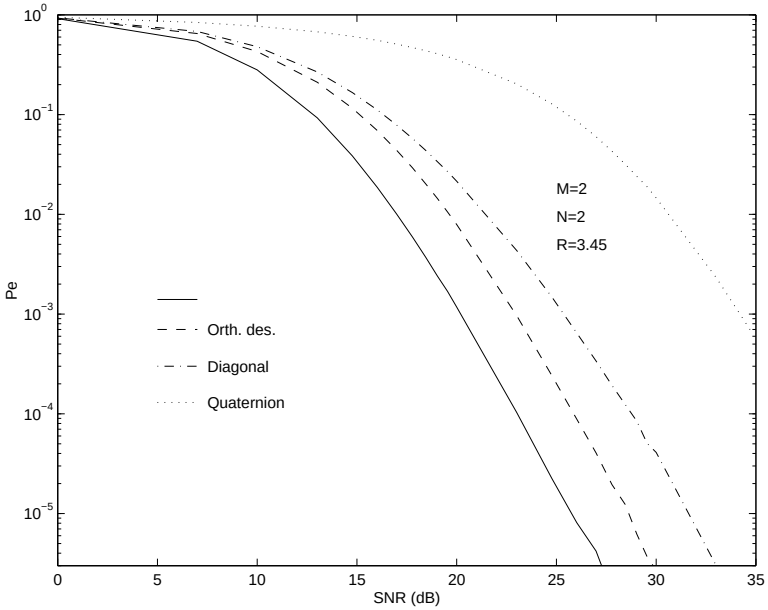
Platonic body in four dimensions, the 120-cell (Notices of the AMS, January 2000).

Performance

$\zeta(SL_2(\mathbb{F}_5)) \sim 0.309.$

Excellent performance in simulations.





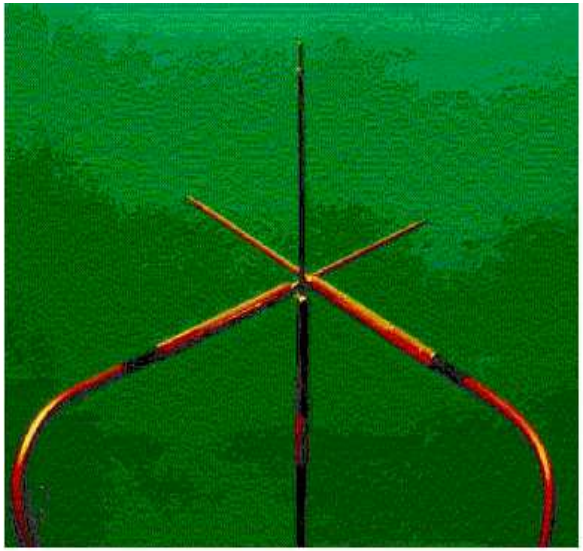
All Groups

IEEE IT September 2001:

Group type	order	dim of rep
$G_{m,r}$	mn	n
$D_{m,r,\ell}$	$2mn$	$2n$
E_m	$24m$	2
$F_{m,r}$	$2mn$	$2n$
$H_{m,\ell}$	$48m$	4
$\mathsf{SL}_2(\mathbb{F}_5)$	120	2
$K_{m,r,\ell}$	$240mn$	$4n$
$U \times H$	$\lvert U\rvert\lvert H\rvert$	$\dim(U)\dim(H)$

Practical

The group $G_{21,4}$ with 63 elements is being used on a prototypical 3-antenna constellation in the Bell Labs hallways. (Mike Andrews)



Further Work

- Optimization of 2-dimensional diagonal codes and Fibonacci numbers (S-2001)

- Good, not fully diverse groups, using character tables (S-2001)

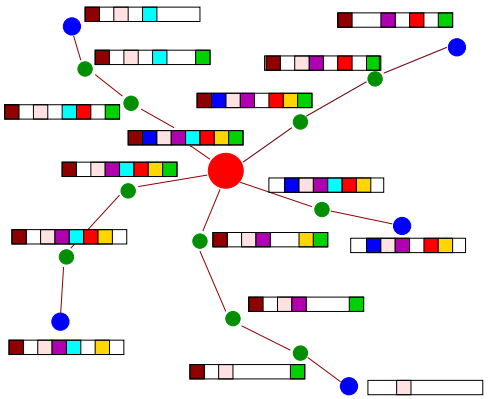
- Good modulation schemes from representations of compact Lie groups. (S-2001).

Codes and Efficient Content Delivery

Goal: Delivering popular content to many receivers.

Problem: Reliability. The common TCP/IP protocol is not scalable to many receivers.

Reason: TCP/IP requires feedback from receivers on lost packets.



Solution: Encode the content in such a way that recovery is possible if some packets are lost.

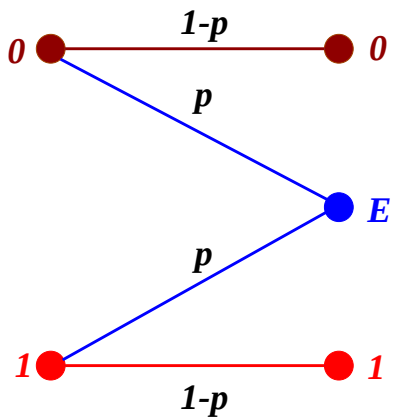
Codes

A linear code over the field $\mathbb{F}_q$ of block-length n and dimension k is a k-dimensioal linear subspace of $\mathbb{F}_q^n$. The fraction k/n is called the *rate* of the code.

Typically, we assume that $q = 2$. In this case, the code is called binary.

Philosophy: Add redundant information ($n - k$ redundant coordinate positions) as to be able to correct errors.

What errors to correct? Erasures:

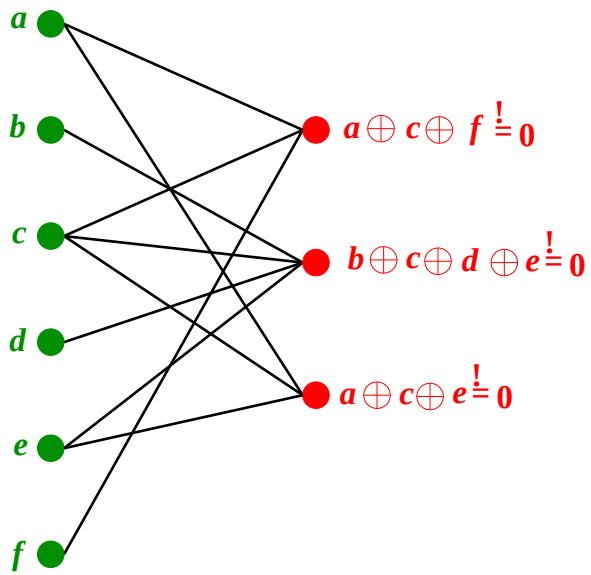


Code Requirements

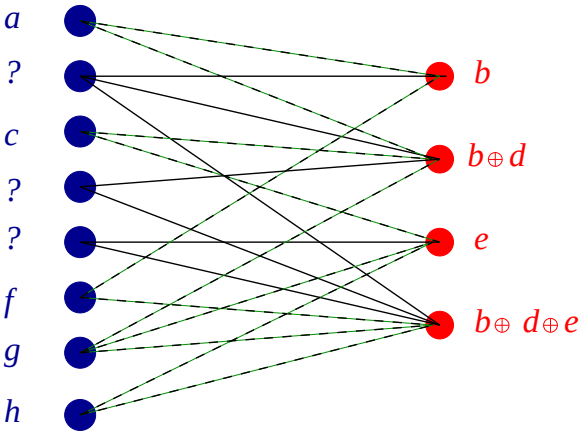
Want codes with fast encoding and decoding algorithms.

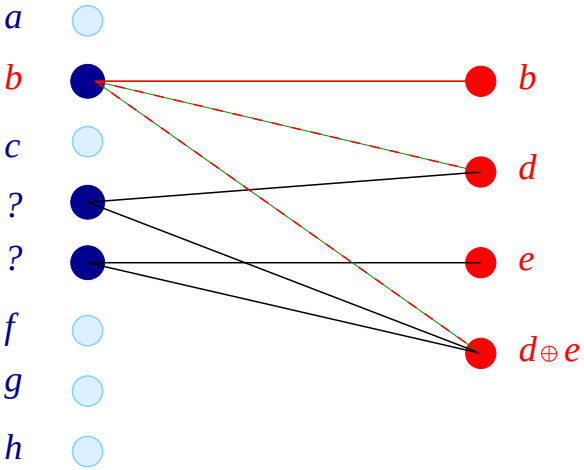
Reed-Solomon codes: Optimal, but slow.

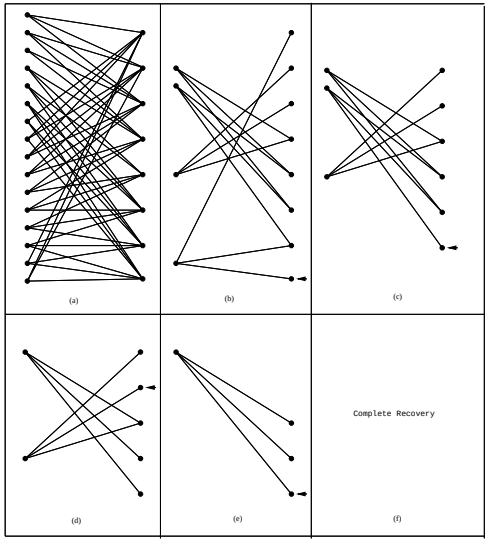
LDPC codes: Built from sparse graphs



Decoding

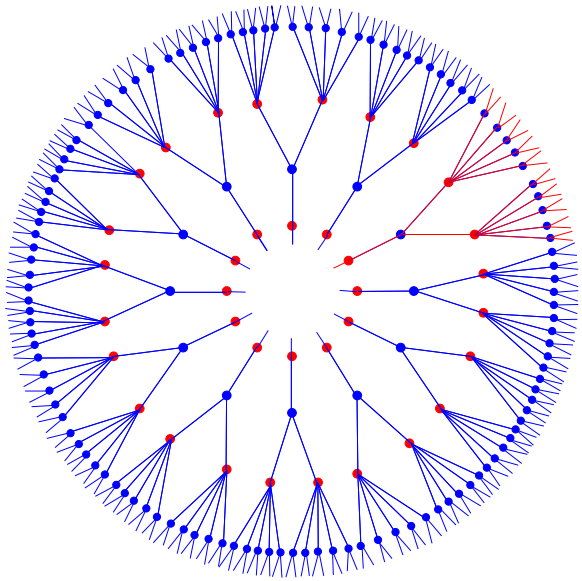


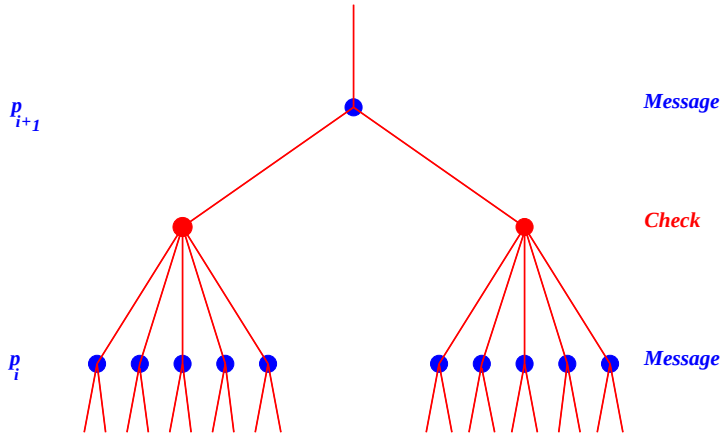




Decoding time is proportional to number of edges in the graph. Condition for successful decoding?

The Tree Analysis





Succesful decoding depends only on the degree distribution generating functions $\lambda(x)$ and $\rho(x)$ of the message and check nodes:

$$p\lambda(1-\rho(1-x)) < x \qquad \text{for } x \in (0,p).$$

Tree analysis produces recursion for the expected fraction of erased nodes at each step. Martingale arguments show concentration around expectation.

Code Design: Tornado Codes

For a given rate R design $\lambda(x)$ and $\rho(x)$ such that maximum fraction of tolerable erasures is arbitrarily close to its upper limit $1 - R$.

Choose design parameter D.

$$\lambda(x) := \frac{1}{H(D)}\left(x + \frac{x^2}{2} + \cdots + \frac{x^D}{D}\right)$$

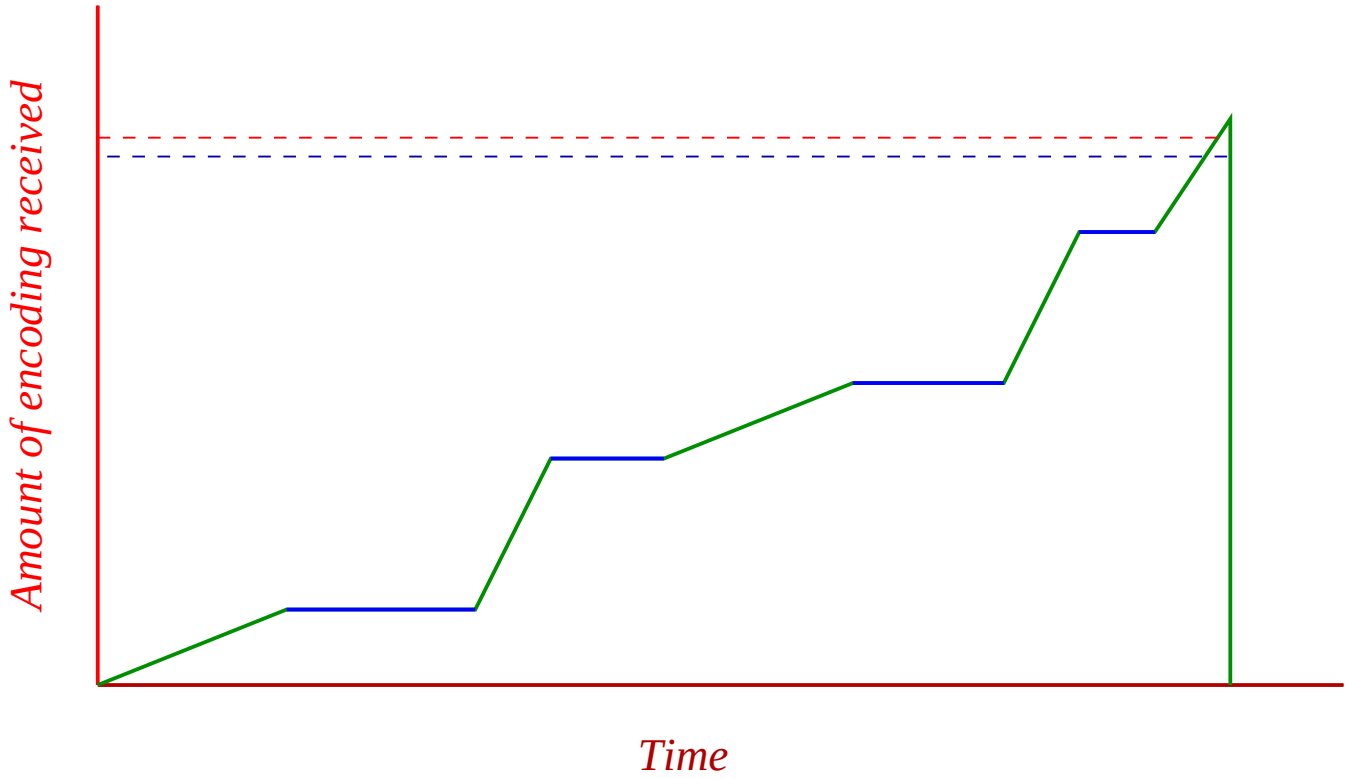
$$\rho(x) := \exp\left(\mu(x-1)\right),$$

where $H(D)$ is the harmonic sum and $\mu = H(D)/\left(1 - 1/(D+1)\right)$.

Given D, decoding can be done in time $O(n \log(1/D))$, where n is the block-length.

Tornado codes achieve capacity on the erasure channel.

Protocol

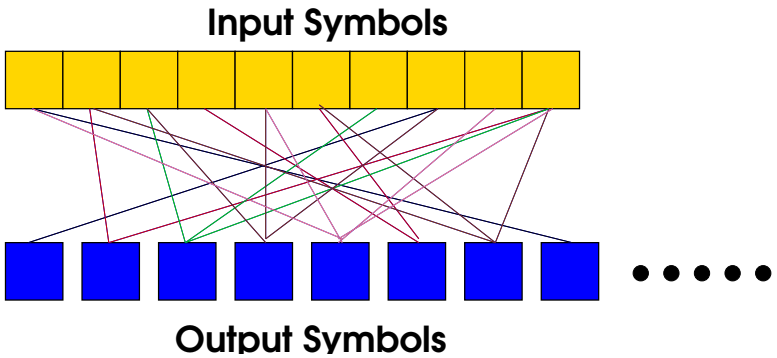


Beyond Tornado

Traditional codes are not practical for building a data transmission system, since the loss rate of individual receivers has to be estimated prior to transmission.

Need *universal* codes that achieve capacity *simultaneously* for any finite number of erasure channels.

LT-codes:



LT-Codes

Occupancy problem: average weight of output nodes is $\Omega(\log(K))$, where n is number of input symbols.

LT-codes have average weight $O(\log(K))$, and have encoding/decoding time $O(K \log(K))$.

Theory is different from Tornado codes.