

Large Codes and Weil Numbers

Bernhard Schmidt

Nanyang Technological University

Joint work with Dang Khoa Nguyen

A binary linear recursion

$$a_i = a_{i-1} + a_{i-8} + a_{i-11} + a_{i-15} \pmod{2}$$

- Need initial values a_0, \dots, a_{14} (input)
- Period length : 1057
- Weight of a period : $\sum_{i=0}^{1056} a_i$

Weights of periods for 100 random inputs

540	540	520	544	540	484	540	544	532	484
544	504	504	532	540	532	532	504	540	484
544	484	540	540	520	544	540	504	520	540
504	544	532	520	544	544	544	540	532	532
540	540	484	520	540	504	540	540	532	544
504	540	540	532	504	520	544	540	540	540
540	504	544	520	540	544	540	540	532	520
484	520	544	532	504	532	504	532	520	540
540	544	532	504	544	544	544	532	504	532
540	520	544	540	540	540	520	532	532	520

Occurring weights : 484, 504, 520, 532, 540, 544

Gauss Sums

- $\text{GF}(2^k)$: finite field of order 2^k
- $\chi : \text{GF}(2^k)^* \rightarrow \mathbf{C}$ multiplicative character
- $\text{Tr} : \text{GF}(2^k) \rightarrow \{0,1\}$ absolute trace

$$G(\chi) = \sum_{x \in \text{GF}(2^k)} (-1)^{\text{Tr}(x)} \chi(x)$$

A Gauss sum over $\text{GF}(2^{15})$

- $\zeta = \exp(2\pi i/31)$
- g : primitive element of $\text{GF}(2^{15})$
- $\chi : \text{GF}(2^{15})^* \rightarrow \mathbf{C}, \quad \chi(g) = \zeta$

Value of $G(\chi)$:

$24\zeta^{28}$	$+56\zeta^{26}$	$+24\zeta^{25}$	$-24\zeta^{24}$	$+56\zeta^{22}$	$+56\zeta^{21}$	$-16\zeta^{20}$
$+24\zeta^{19}$	$-16\zeta^{18}$	$-24\zeta^{17}$	$-16\zeta^{16}$	$+24\zeta^{14}$	$+56\zeta^{13}$	$-24\zeta^{12}$
$+56\zeta^{11}$	$-16\zeta^{10}$	$-16\zeta^9$	$-16\zeta^8$	$+24\zeta^7$	$-24\zeta^6$	$-16\zeta^5$
$-16\zeta^4$	$-24\zeta^3$	$-16\zeta^2$	-16ζ	$+96$		

$$-G(\chi) / 2$$

"Normalized" value of $-G(\chi) / 2$:

$532 \zeta^{30}$	$+532 \zeta^{29}$	$+520 \zeta^{28}$	$+532 \zeta^{27}$	$+504 \zeta^{26}$	$+520 \zeta^{25}$
$+544 \zeta^{24}$	$+532 \zeta^{23}$	$+504 \zeta^{22}$	$+504 \zeta^{21}$	$+540 \zeta^{20}$	$+520 \zeta^{19}$
$+540 \zeta^{18}$	$+544 \zeta^{17}$	$+540 \zeta^{16}$	$+532 \zeta^{15}$	$+520 \zeta^{14}$	$+504 \zeta^{13}$
$+544 \zeta^{12}$	$+504 \zeta^{11}$	$+540 \zeta^{10}$	$+540 \zeta^9$	$+540 \zeta^8$	$+520 \zeta^7$
$+544 \zeta^6$	$+540 \zeta^5$	$+540 \zeta^4$	$+544 \zeta^3$	$+540 \zeta^2$	$+540 \zeta$
$+484$					

Recall : weights from in binary recursion are

484, 504, 520, 532, 540, 544

An irreducible cyclic code

- θ : primitive 1057th root of unity in $GF(2^{15})$
- Tr : absolute trace $GF(2^{15}) \rightarrow GF(2)$
- $c(x) = (\text{Tr}(x), \text{Tr}(x\theta), \dots, \text{Tr}(x\theta^{1056}))$
- $C = \{c(x) : x \in GF(2^{15})\}$: cyclic (1057,15) code

Weights?

Code \rightarrow recursion

- $c(x) = (\text{Tr}(x), \text{Tr}(x\theta), \dots, \text{Tr}(x\theta^{1056}))$
- Entries : $c_i = \text{Tr}(x\theta^i)$
- Minimum polynomial over GF(2) : $m_\theta = x^{15} + x^{14} + x^7 + x^4 + 1$

$$c_{i+15} + c_{i+14} + c_{i+7} + c_{i+4} + c_i$$

$$= \text{Tr}(x\theta^{i+15}) + \text{Tr}(x\theta^{i+14}) + \text{Tr}(x\theta^{i+7}) + \text{Tr}(x\theta^{i+4}) + \text{Tr}(x\theta^i)$$

$$= \text{Tr}(x(\theta^{i+15} + \theta^{i+14} + \theta^{i+7} + \theta^{i+4} + \theta^i))$$

$$= 0$$

Weights

$$c_{i+15} + c_{i+14} + c_{i+7} + c_{i+4} + c_i = 0 \Rightarrow c_i = c_{i-1} + c_{i-8} + c_{i-11} + c_{i-15}$$

- Codewords are exactly the solutions of binary recursion
- 484, 504, 520, 532, 540, 544 are the nonzero weights of code
- Need to understand : Gauss sum \leftrightarrow weights of code

Gauss sum \leftrightarrow weights

- $2^{15} - 1 = 31 \cdot 1057$
- g primitive element of $\text{GF}(2^{15})$, $\theta = g^{31}$
- $\chi(g) = \exp(2\pi i / 31) =: \zeta$

$$G(\chi) = \sum_{x \in \text{GF}(2^{15})} (-1)^{\text{Tr}(x)} \chi(x) = \sum_{j=0}^{30} \sum_{i=0}^{1056} (-1)^{\text{Tr}(g^j \theta^i)} \chi(g^j \theta^i) =$$

$$\sum_{j=0}^{30} \chi(g^j) \sum_{i=0}^{1056} (-1)^{\text{Tr}(g^j \theta^i)} = \sum_{j=0}^{30} \zeta^j (1057 - 2 \cdot \text{weight}(c(g^j)))$$

Weil numbers

- $\zeta = \exp(2\pi i / e)$, n positive **integer**
- $X \in \mathbf{Z}[\zeta]$ is n -**Weil number** if $X \overline{X} = n$
- Gauss sums over $\text{GF}(q)$ are q -Weil numbers
- abelian difference sets \rightarrow Weil numbers
- Baumert's sieve : difference sets and weight distributions of codes can be "constructed" from Weil numbers

Problem:

Weil numbers can only be computed in "easy" cases

"Easy" Weil numbers and ideals

$$\zeta = \exp(2\pi i / e), \quad X \in \mathbf{Z}[\zeta], \quad X \bar{X} = n$$

- Gauss sums over $\text{GF}(q)$ can be computed for $q < 10^{15}$
- Ideal equation in $\mathbf{Z}[\zeta]$: $I\bar{I} = n\mathbf{Z}[\zeta]$
- All n -Weil numbers can be found if
 - there are only few solutions of the ideal equation
 - the solutions which are principal ideals can be filtered out
 - generators for the principal solutions can be found
 - usually means $n\mathbf{Z}[\zeta]$ divisible by less than 10 prime ideals

Some hope : Weil numbers are rare

- $R := \bigcup_{e \geq 1} \mathbf{Z}[\zeta_e]$
- n : fixed positive integer

Conjecture(Kedlaya 2001)

Up to multiplication with roots of unity there are only finitely many n - Weil numbers in R

- proved for $\bigcup_{e \text{ prime}} \mathbf{Z}[\zeta_e]$ instead of R

Weil numbers and lattices

$$\zeta = \exp(2\pi i / e), \quad X \in \mathbf{Z}[\zeta], \quad X \bar{X} = n$$

- Ideal $X\mathbf{Z}[\zeta]$ is free \mathbf{Z} -submodule of $\mathbf{Z}[\zeta]$ of rank $\varphi(e)$
- B : \mathbf{Z} -basis of $X\mathbf{Z}[\zeta]$
- $L: B \rightarrow \mathbf{R}, (b_1, b_2) \mapsto \text{Tr}(b_1 \bar{b}_2)$
- extend L to bilinear form on vector space $X\mathbf{Z}[\zeta] \otimes \mathbf{R}$

$X\mathbf{Z}[\zeta] \otimes \mathbf{R}$ and L form a **lattice**

Weil numbers and lattices

$$X \in \mathbf{Z}[\zeta_e], \quad X \bar{X} = n, \quad \alpha X \in X\mathbf{Z}[\zeta_e] \text{ arbitrary}$$

$$\mathrm{Tr}(\alpha X \overline{\alpha X}) = n \mathrm{Tr}(\alpha \bar{\alpha}) = n \sum_{\sigma \in G} (\alpha \bar{\alpha})^\sigma = n \sum_{\sigma \in G} |\alpha^\sigma|^2$$

$$\text{side condition : } \prod_{\sigma \in G} |\alpha^\sigma|^2 = \prod_{\sigma \in G} (\alpha \bar{\alpha})^\sigma = N(\alpha)^2 \geq 1$$

$$\mathrm{Tr}(\alpha X \overline{\alpha X}) \geq n/G, \quad \text{equality} \Leftrightarrow \alpha = \pm \zeta_e^i$$

X shortest vector in lattice $X\mathbf{Z}[\zeta_e]$

(H.W. Lenstra, P. van Wamelen)

Computing Weil numbers via shortest vectors

Shortest vectors in lattices can be enumerated by Fincke-Pohst algorithm
Obstacles:

1. Find generators of $X\mathbf{Z}[\zeta_e]$ without knowing X
2. Must work in subfield of $\mathbf{Q}(\zeta_e)$
3. Find integral basis for subfield
4. Find generators for $X\mathbf{Z}[\zeta_e]$ in subfield
5. Find \mathbf{Z} -basis of $X\mathbf{Z}[\zeta_e]$ in subfield
6. Fincke - Pohst exponential time in dimension of lattice

Computation of a Gauss sum

- $\chi: \text{GF}(2^{121})^* \rightarrow \mathbf{C}$ character of order 727
- $G(\chi) = \sum_{x \in \text{GF}(2^{121})} (-1)^{\text{Tr}(x)} \chi(x)$
- $2^{121} \cong 2.7 \cdot 10^{36} \rightarrow$ naively summing up impossible
- We try the shortest vector approach

Problem 1:

Find generators of $X\mathbf{Z}[\zeta_e]$ without knowing X

- Here $X = G(\chi) = \sum_{x \in \text{GF}(2^{121})} (-1)^{\text{Tr}(x)} \chi(x)$
- Stickelberger : $G(\chi)\mathbf{Z}[\zeta_e] = P_1^{62} P_2^{66} P_3^{58} P_4^{59} P_5^{55} P_6^{63}$
- Kummer : $P_1 = (2, f(\zeta))$

$$f(\zeta) = \zeta^{121} + \zeta^{120} + \zeta^{116} + \zeta^{114} + \zeta^{113} + \zeta^{112} + \zeta^{111} + \zeta^{109} + \zeta^{107} + \zeta^{106} + \zeta^{103} + \zeta^{99} + \zeta^{97} + \zeta^{96} + \zeta^{94} + \zeta^{91} + \zeta^{90} + \zeta^{89} + \zeta^{87} + \zeta^{86} + \zeta^{85} + \zeta^{83} + \zeta^{82} + \zeta^{81} + \zeta^{80} + \zeta^{79} + \zeta^{78} + \zeta^{77} + \zeta^{76} + \zeta^{74} + \zeta^{73} + \zeta^{72} + \zeta^{71} + \zeta^{68} + \zeta^{67} + \zeta^{66} + \zeta^{63} + \zeta^{61} + \zeta^{60} + \zeta^{58} + \zeta^{57} + \zeta^{55} + \zeta^{54} + \zeta^{51} + \zeta^{50} + \zeta^{47} + \zeta^{44} + \zeta^{43} + \zeta^{38} + \zeta^{37} + \zeta^{36} + \zeta^{35} + \zeta^{34} + \zeta^{30} + \zeta^{29} + \zeta^{28} + \zeta^{27} + \zeta^{25} + \zeta^{24} + \zeta^{23} + \zeta^{22} + \zeta^{21} + \zeta^{18} + \zeta^{17} + \zeta^{16} + \zeta^{15} + \zeta^{13} + \zeta^{12} + \zeta^9 + \zeta^8 + \zeta^7 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1$$

Problem 2:

Must work in subfield of $\mathbf{Q}(\zeta_e)$

- Here $[\mathbf{Q}(\zeta_e) : \mathbf{Q}] = \varphi(727) = 726$

- Too large for Fincke - Pohst

- Property of Gauss sums :

$$G(\chi)^{\sigma_2} = G(\chi), \quad \sigma_2 : \zeta_{727} \mapsto (\zeta_{727})^2$$

- Can work in $\text{Fix}(\sigma_2)$

- $[\text{Fix}(\sigma_2) : \mathbf{Q}] = \varphi(727) / \text{ord}_{727}(2) = 6$

Problem 3:

Find integral basis for subfield

- Algorithms for general number fields inappropriate
- Use integral bases constructed by Breuer/Zumbroich (1995)
- Basis elements expressed as polynomials in ζ_e
- Ideally suited for computations
- For e prime, Gaussian periods can be used:

$$\eta_i = \sum_{j=0}^{\text{ord}_e(2)-1} \zeta_e^{2^j a^i}, \quad (\mathbf{Z}/e\mathbf{Z})^* = \langle a \rangle$$

Problem 3:

Find integral basis for subfield, case $e = 727$

$$\begin{aligned} &\zeta^{724} + \zeta^{721} + \zeta^{716} + \zeta^{715} + \zeta^{705} + \zeta^{703} + \zeta^{700} + \zeta^{686} + \zeta^{683} + \zeta^{679} + \zeta^{673} + \zeta^{662} + \zeta^{658} + \\ &\zeta^{648} + \zeta^{645} + \zeta^{639} + \zeta^{631} + \zeta^{628} + \zeta^{619} + \zeta^{602} + \zeta^{597} + \zeta^{594} + \zeta^{590} + \zeta^{589} + \zeta^{576} + \zeta^{569} + \\ &\zeta^{568} + \zeta^{563} + \zeta^{551} + \zeta^{535} + \zeta^{529} + \zeta^{528} + \zeta^{514} + \zeta^{512} + \zeta^{511} + \zeta^{492} + \zeta^{484} + \zeta^{482} + \zeta^{477} + \\ &\zeta^{474} + \zeta^{467} + \zeta^{461} + \zeta^{454} + \zeta^{453} + \zeta^{451} + \zeta^{442} + \zeta^{425} + \zeta^{424} + \zeta^{414} + \zeta^{411} + \zeta^{409} + \zeta^{404} + \\ &\zeta^{399} + \zeta^{390} + \zeta^{380} + \zeta^{375} + \zeta^{368} + \zeta^{364} + \zeta^{362} + \zeta^{358} + \zeta^{350} + \zeta^{343} + \zeta^{331} + \zeta^{329} + \zeta^{324} + \\ &\zeta^{314} + \zeta^{301} + \zeta^{297} + \zeta^{295} + \zeta^{288} + \zeta^{284} + \zeta^{264} + \zeta^{257} + \zeta^{256} + \zeta^{246} + \zeta^{242} + \zeta^{241} + \zeta^{237} + \\ &\zeta^{227} + \zeta^{221} + \zeta^{212} + \zeta^{207} + \zeta^{202} + \zeta^{195} + \zeta^{190} + \zeta^{184} + \zeta^{182} + \zeta^{181} + \zeta^{179} + \zeta^{175} + \zeta^{162} + \\ &\zeta^{157} + \zeta^{144} + \zeta^{142} + \zeta^{132} + \zeta^{128} + \zeta^{123} + \zeta^{121} + \zeta^{106} + \zeta^{101} + \zeta^{95} + \zeta^{92} + \zeta^{91} + \zeta^{81} + \zeta^{72} + \\ &\zeta^{71} + \zeta^{66} + \zeta^{64} + \zeta^{53} + \zeta^{46} + \zeta^{36} + \zeta^{33} + \zeta^{32} + \zeta^{23} + \zeta^{18} + \zeta^{16} + \zeta^9 + \zeta^8 + \zeta^4 + \zeta^2 + \zeta \end{aligned}$$

$$\begin{aligned} &\zeta^{720} + \zeta^{713} + \zeta^{712} + \zeta^{710} + \zeta^{699} + \zeta^{697} + \zeta^{693} + \zeta^{672} + \zeta^{671} + \zeta^{667} + \zeta^{666} + \zeta^{664} + \zeta^{660} + \\ &\zeta^{659} + \zeta^{640} + \zeta^{634} + \zeta^{617} + \zeta^{616} + \zeta^{615} + \zeta^{607} + \zeta^{605} + \zeta^{601} + \zeta^{593} + \zeta^{592} + \zeta^{591} + \zeta^{574} + \\ &\zeta^{566} + \zeta^{558} + \zeta^{553} + \zeta^{541} + \zeta^{530} + \zeta^{522} + \zeta^{507} + \zeta^{505} + \zeta^{503} + \zeta^{496} + \zeta^{494} + \zeta^{487} + \zeta^{483} + \\ &\zeta^{478} + \zeta^{475} + \zeta^{464} + \zeta^{460} + \zeta^{459} + \zeta^{458} + \zeta^{457} + \zeta^{455} + \zeta^{446} + \zeta^{421} + \zeta^{408} + \zeta^{405} + \zeta^{402} + \\ &\zeta^{389} + \zeta^{386} + \zeta^{382} + \zeta^{379} + \zeta^{378} + \zeta^{374} + \zeta^{366} + \zeta^{360} + \zeta^{356} + \zeta^{355} + \zeta^{336} + \zeta^{333} + \zeta^{332} + \\ &\zeta^{330} + \zeta^{320} + \zeta^{317} + \zeta^{308} + \zeta^{296} + \zeta^{287} + \zeta^{283} + \zeta^{279} + \zeta^{265} + \zeta^{261} + \zeta^{248} + \zeta^{247} + \zeta^{239} + \\ &\zeta^{232} + \zeta^{230} + \zeta^{229} + \zeta^{223} + \zeta^{204} + \zeta^{201} + \zeta^{193} + \zeta^{191} + \zeta^{189} + \zeta^{187} + \zeta^{183} + \zeta^{180} + \zeta^{178} + \\ &\zeta^{168} + \zeta^{166} + \zeta^{165} + \zeta^{160} + \zeta^{154} + \zeta^{148} + \zeta^{124} + \zeta^{116} + \zeta^{115} + \zeta^{102} + \zeta^{90} + \zeta^{89} + \zeta^{84} + \zeta^{83} + \\ &\zeta^{80} + \zeta^{77} + \zeta^{74} + \zeta^{62} + \zeta^{58} + \zeta^{51} + \zeta^{45} + \zeta^{42} + \zeta^{40} + \zeta^{37} + \zeta^{31} + \zeta^{29} + \zeta^{21} + \zeta^{20} + \zeta^{10} + \zeta^5 \end{aligned}$$

$$\begin{aligned} &\zeta^{708} + \zeta^{692} + \zeta^{689} + \zeta^{688} + \zeta^{668} + \zeta^{657} + \zeta^{652} + \zeta^{651} + \zeta^{649} + \zeta^{642} + \zeta^{620} + \zeta^{609} + \\ &\zeta^{598} + \zeta^{587} + \zeta^{586} + \zeta^{584} + \zeta^{580} + \zeta^{578} + \zeta^{577} + \zeta^{575} + \zeta^{571} + \zeta^{557} + \zeta^{556} + \zeta^{524} + \\ &\zeta^{513} + \zeta^{510} + \zeta^{508} + \zeta^{491} + \zeta^{476} + \zeta^{469} + \zeta^{468} + \zeta^{456} + \zeta^{452} + \zeta^{450} + \zeta^{447} + \zeta^{445} + \\ &\zeta^{441} + \zeta^{436} + \zeta^{433} + \zeta^{429} + \zeta^{427} + \zeta^{423} + \zeta^{422} + \zeta^{420} + \zeta^{418} + \zeta^{416} + \zeta^{415} + \zeta^{412} + \\ &\zeta^{400} + \zeta^{392} + \zeta^{388} + \zeta^{387} + \zeta^{385} + \zeta^{376} + \zeta^{370} + \zeta^{354} + \zeta^{346} + \zeta^{344} + \zeta^{334} + \zeta^{326} + \\ &\zeta^{321} + \zeta^{310} + \zeta^{299} + \zeta^{293} + \zeta^{292} + \zeta^{290} + \zeta^{289} + \zeta^{278} + \zeta^{262} + \zeta^{255} + \zeta^{254} + \zeta^{238} + \\ &\zeta^{234} + \zeta^{228} + \zeta^{226} + \zeta^{225} + \zeta^{218} + \zeta^{211} + \zeta^{210} + \zeta^{209} + \zeta^{208} + \zeta^{206} + \zeta^{200} + \zeta^{196} + \\ &\zeta^{194} + \zeta^{188} + \zeta^{185} + \zeta^{177} + \zeta^{173} + \zeta^{172} + \zeta^{167} + \zeta^{163} + \zeta^{155} + \zeta^{146} + \zeta^{145} + \zeta^{139} + \\ &\zeta^{131} + \zeta^{127} + \zeta^{119} + \zeta^{117} + \zeta^{114} + \zeta^{113} + \zeta^{109} + \zeta^{105} + \zeta^{104} + \zeta^{103} + \zeta^{100} + \zeta^{98} + \\ &\zeta^{97} + \zeta^{94} + \zeta^{86} + \zeta^{73} + \zeta^{57} + \zeta^{52} + \zeta^{50} + \zeta^{49} + \zeta^{47} + \zeta^{43} + \zeta^{26} + \zeta^{25} + \zeta^{13} \end{aligned}$$

$$\begin{aligned} &\zeta^{726} + \zeta^{725} + \zeta^{723} + \zeta^{719} + \zeta^{718} + \zeta^{711} + \zeta^{709} + \zeta^{704} + \zeta^{695} + \zeta^{694} + \zeta^{691} + \zeta^{681} + \zeta^{674} + \\ &\zeta^{663} + \zeta^{661} + \zeta^{656} + \zeta^{655} + \zeta^{646} + \zeta^{636} + \zeta^{635} + \zeta^{632} + \zeta^{626} + \zeta^{621} + \zeta^{606} + \zeta^{604} + \zeta^{599} + \\ &\zeta^{595} + \zeta^{585} + \zeta^{583} + \zeta^{570} + \zeta^{565} + \zeta^{552} + \zeta^{548} + \zeta^{546} + \zeta^{545} + \zeta^{543} + \zeta^{537} + \zeta^{532} + \zeta^{525} + \\ &\zeta^{520} + \zeta^{515} + \zeta^{506} + \zeta^{500} + \zeta^{490} + \zeta^{486} + \zeta^{485} + \zeta^{481} + \zeta^{471} + \zeta^{470} + \zeta^{463} + \zeta^{443} + \zeta^{439} + \\ &\zeta^{432} + \zeta^{430} + \zeta^{426} + \zeta^{413} + \zeta^{403} + \zeta^{398} + \zeta^{396} + \zeta^{384} + \zeta^{377} + \zeta^{369} + \zeta^{365} + \zeta^{363} + \zeta^{359} + \\ &\zeta^{352} + \zeta^{347} + \zeta^{337} + \zeta^{328} + \zeta^{323} + \zeta^{318} + \zeta^{316} + \zeta^{313} + \zeta^{303} + \zeta^{302} + \zeta^{285} + \zeta^{276} + \zeta^{274} + \\ &\zeta^{273} + \zeta^{266} + \zeta^{260} + \zeta^{253} + \zeta^{250} + \zeta^{245} + \zeta^{243} + \zeta^{235} + \zeta^{216} + \zeta^{215} + \zeta^{213} + \zeta^{199} + \zeta^{198} + \\ &\zeta^{192} + \zeta^{176} + \zeta^{164} + \zeta^{159} + \zeta^{158} + \zeta^{151} + \zeta^{138} + \zeta^{137} + \zeta^{133} + \zeta^{130} + \zeta^{125} + \zeta^{108} + \zeta^{99} + \zeta^{96} + \\ &\zeta^{88} + \zeta^{82} + \zeta^{79} + \zeta^{69} + \zeta^{65} + \zeta^{54} + \zeta^{48} + \zeta^{44} + \zeta^{41} + \zeta^{27} + \zeta^{24} + \zeta^{22} + \zeta^{12} + \zeta^{11} + \zeta^6 + \zeta^3 \end{aligned}$$

$$\begin{aligned} &\zeta^{722} + \zeta^{717} + \zeta^{707} + \zeta^{706} + \zeta^{698} + \zeta^{696} + \zeta^{690} + \zeta^{687} + \zeta^{685} + \zeta^{682} + \zeta^{676} + \zeta^{669} + \\ &\zeta^{665} + \zeta^{653} + \zeta^{650} + \zeta^{647} + \zeta^{644} + \zeta^{643} + \zeta^{638} + \zeta^{637} + \zeta^{625} + \zeta^{612} + \zeta^{611} + \zeta^{603} + \\ &\zeta^{579} + \zeta^{573} + \zeta^{567} + \zeta^{562} + \zeta^{561} + \zeta^{559} + \zeta^{549} + \zeta^{547} + \zeta^{544} + \zeta^{540} + \zeta^{538} + \zeta^{536} + \\ &\zeta^{534} + \zeta^{526} + \zeta^{523} + \zeta^{504} + \zeta^{498} + \zeta^{497} + \zeta^{495} + \zeta^{488} + \zeta^{480} + \zeta^{479} + \zeta^{466} + \zeta^{462} + \\ &\zeta^{448} + \zeta^{444} + \zeta^{440} + \zeta^{431} + \zeta^{419} + \zeta^{410} + \zeta^{407} + \zeta^{397} + \zeta^{395} + \zeta^{394} + \zeta^{391} + \zeta^{372} + \\ &\zeta^{371} + \zeta^{367} + \zeta^{361} + \zeta^{353} + \zeta^{340} + \zeta^{348} + \zeta^{345} + \zeta^{341} + \zeta^{338} + \zeta^{325} + \zeta^{322} + \zeta^{319} + \\ &\zeta^{306} + \zeta^{281} + \zeta^{272} + \zeta^{270} + \zeta^{269} + \zeta^{268} + \zeta^{267} + \zeta^{263} + \zeta^{252} + \zeta^{249} + \zeta^{244} + \zeta^{240} + \\ &\zeta^{233} + \zeta^{231} + \zeta^{224} + \zeta^{222} + \zeta^{220} + \zeta^{205} + \zeta^{197} + \zeta^{186} + \zeta^{174} + \zeta^{169} + \zeta^{161} + \zeta^{153} + \\ &\zeta^{136} + \zeta^{135} + \zeta^{134} + \zeta^{126} + \zeta^{122} + \zeta^{120} + \zeta^{112} + \zeta^{111} + \zeta^{110} + \zeta^{93} + \zeta^{87} + \zeta^{68} + \\ &\zeta^{67} + \zeta^{63} + \zeta^{61} + \zeta^{60} + \zeta^{56} + \zeta^{55} + \zeta^{34} + \zeta^{30} + \zeta^{28} + \zeta^{17} + \zeta^{15} + \zeta^{14} + \zeta^7 \end{aligned}$$

$$\begin{aligned} &\zeta^{714} + \zeta^{702} + \zeta^{701} + \zeta^{684} + \zeta^{680} + \zeta^{678} + \zeta^{677} + \zeta^{675} + \zeta^{670} + \zeta^{654} + \zeta^{641} + \zeta^{633} + \\ &\zeta^{630} + \zeta^{629} + \zeta^{627} + \zeta^{624} + \zeta^{623} + \zeta^{622} + \zeta^{618} + \zeta^{614} + \zeta^{613} + \zeta^{610} + \zeta^{608} + \zeta^{600} + \\ &\zeta^{596} + \zeta^{588} + \zeta^{582} + \zeta^{581} + \zeta^{572} + \zeta^{564} + \zeta^{560} + \zeta^{555} + \zeta^{554} + \zeta^{550} + \zeta^{542} + \zeta^{539} + \\ &\zeta^{533} + \zeta^{531} + \zeta^{527} + \zeta^{521} + \zeta^{519} + \zeta^{518} + \zeta^{517} + \zeta^{516} + \zeta^{509} + \zeta^{502} + \zeta^{501} + \zeta^{499} + \\ &\zeta^{493} + \zeta^{489} + \zeta^{473} + \zeta^{472} + \zeta^{465} + \zeta^{449} + \zeta^{438} + \zeta^{437} + \zeta^{435} + \zeta^{434} + \zeta^{428} + \zeta^{417} + \\ &\zeta^{406} + \zeta^{401} + \zeta^{393} + \zeta^{383} + \zeta^{381} + \zeta^{373} + \zeta^{357} + \zeta^{351} + \zeta^{342} + \zeta^{340} + \zeta^{339} + \zeta^{335} + \\ &\zeta^{327} + \zeta^{315} + \zeta^{312} + \zeta^{311} + \zeta^{309} + \zeta^{307} + \zeta^{305} + \zeta^{304} + \zeta^{300} + \zeta^{298} + \zeta^{294} + \zeta^{291} + \\ &\zeta^{286} + \zeta^{282} + \zeta^{280} + \zeta^{277} + \zeta^{275} + \zeta^{271} + \zeta^{259} + \zeta^{258} + \zeta^{251} + \zeta^{236} + \zeta^{219} + \zeta^{217} + \\ &\zeta^{214} + \zeta^{203} + \zeta^{171} + \zeta^{170} + \zeta^{156} + \zeta^{152} + \zeta^{150} + \zeta^{149} + \zeta^{147} + \zeta^{143} + \zeta^{141} + \zeta^{140} + \\ &\zeta^{129} + \zeta^{118} + \zeta^{107} + \zeta^{85} + \zeta^{78} + \zeta^{76} + \zeta^{75} + \zeta^{70} + \zeta^{59} + \zeta^{39} + \zeta^{38} + \zeta^{35} + \zeta^{19} \end{aligned}$$

Problem 4 :

Find generators for $X\mathbf{Z}[\zeta_e]$ in subfield

- In $\mathbf{Z}[\zeta_e]$: $P_i = (2, f_i(\zeta))$ (Kummer)
- Cannot use Kummer for subfield, no integral power basis!
- Luckily : $P_i = (2, N(f_i(\zeta)))$ (norm relative to subfield)
- But : coefficient explosion

Problem 4 :

Find generators for $X\mathbf{Z}[\zeta_e]$ in subfield

- Total number of digits still $< 10^7$ in reasonable cases
- Subsequent computations do not dramatically increase number of digits

Kummer + norm solves the problem

Problem 5 :

Find \mathbf{Z} -basis of $X\mathbf{Z}[\zeta_e]$ in subfield

- $G(\chi)\mathbf{Z}[\zeta_e] = P_1^{62} P_2^{66} P_3^{58} P_4^{59} P_5^{55} P_6^{63}$
- $P_i = (2, \mathbf{N}(f_i(\zeta)))$
- Integral basis B for subfield from Breuer/Zumbroich
- $\{2\beta : \beta \in B\} \cup \{\mathbf{N}(f_i(\zeta))\beta : \beta \in B\}$ \mathbf{Z} -generators for P_i
- Write coordinates with respect to B into $d \times 2d$ matrix
($d =$ absolute degree of subfield)
- Compute Hermite Normal Form \rightarrow only d \mathbf{Z} -generators for P_i
- Repeat similar process \rightarrow \mathbf{Z} -generators for $G(\chi)\mathbf{Z}[\zeta_e]$

Problem 6:

Fincke - Pohst exponential time in dimension of lattice

- Fincke - Pohst is based on LLL
- LLL already finds a shortest vector for **ALL** examples tested
- Replace Fincke - Pohst by LLL

Application to weight distribution of binary irreducible cyclic codes

Definition of binary irreducible code of length n and dimension k :

- θ : primitive n th root of unity in $\text{GF}(2^k)$
 - $c(x) = (\text{Tr}(x), \text{Tr}(x\theta), \dots, \text{Tr}(x\theta^{n-1}))$
 - $C = \{c(x) : x \in \text{GF}(2^k)\}, |C| = 2^k$
-
- $c(x) \rightarrow c(x\theta) \rightarrow \dots \rightarrow c(x\theta^{n-1}), \# \text{cycles} : N = (2^k - 1) / n$
 - " (k, N) irreducible code"

Associated Gauss sums

- Recall $2^k - 1 = nN$
- χ : character of $\text{GF}(2^k)^*$ of order $e \mid N$
- g : primitive element of $\text{GF}(2^k)$

$$G(\chi) = \sum_{x \in \text{GF}(2^k)} (-1)^{\text{Tr}(x)} \chi(x) = \sum_{j=0}^{N-1} \sum_{i=0}^{n-1} (-1)^{\text{Tr}(g^j \theta^i)} \chi(g^j \theta^i) =$$

$$\sum_{j=0}^{N-1} \chi(g^j) \sum_{i=0}^{n-1} (-1)^{\text{Tr}(g^j \theta^i)} = \sum_{j=0}^{N-1} \zeta^j (n - 2 \cdot \text{weight}(c(g^j)))$$

McEliece, Rumsey (1970)

- Consider (k, N) irreducible code, $2^k - 1 = nN$
- Smallest possible k : $k_0 = \text{ord}_N(2)$
- Result : Weight distribution for any (k, N) code efficiently can be computed from that of the (k_0, N) code
- Proof uses Davenport/Hasse for Gauss sums

Baumert, McEliece (1972)

Result : Table of weight distributions of (k_0, N) codes for $N < 100$

Methods :

- Direct computation of Gauss sums for small k_0
- Values of Gauss sums are known in semiprimitive case
- Computation of Gauss sums in quadratic subfields
- Baumert's sieve

MacWilliams, Seery (1981)

Result : Table of weight distributions of (k, N) codes for $k < 28$

Methods :

- Binary linear recursion
- CRAY -1

Segal, Ward (1986, 1993)

Result : Weight distributions of (k_0, N) codes for $N < 500$

Methods :

- Stickelberger
- Random search for principal ideals in fields of small degree
- Use of fundamental units to resolve unit ambiguity
- Baumert's sieve

Nguyen, S. (2006)

Result : Weight distributions of (k, N) codes for $N < 5000$ and $k < 42$

Methods :

- Kummer + Stickelberger + Norm \rightarrow ideal generators in subfield
- Breuer/Zumbröich + Hermite Normal Form + Linear Systems
 \rightarrow \mathbf{Z} -basis over subfield
- Algebraic numbers as floating point complex numbers
 \rightarrow efficient computation of Gram matrix of lattice
- LLL \rightarrow Gauss sums up to root of unity
- Baumert's sieve
- Implementation of binary recursion at bit level