THE UNIVERSITY of York

Lattice Coding and its Applications in Communications

Alister Burr

University of York

alister.burr@york.ac.uk

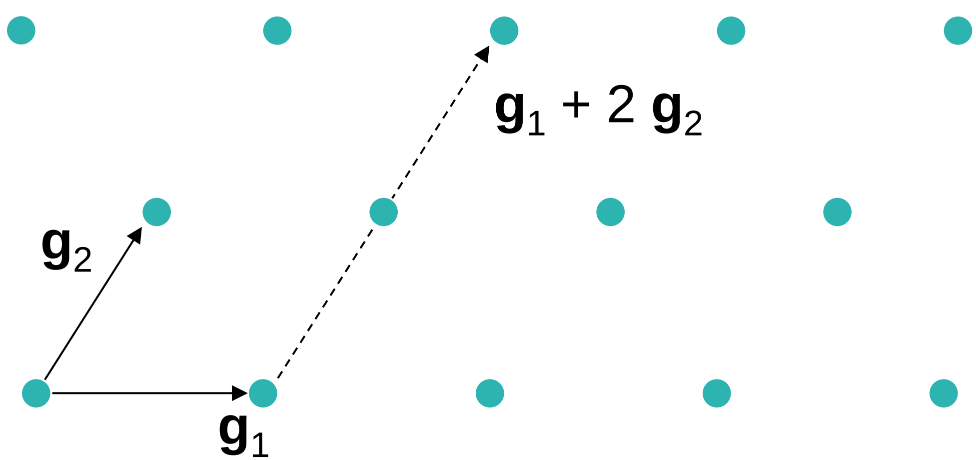
Outline

- Introduction to lattices
  - Definition; Sphere packings; Basis vectors; Matrix description
- Codes and lattice codes
  - Shaping region; Nested lattices
- Lattice constructions
  - Construction A/D, LDLC codes; construction from Gaussian/Eisenstein integers
- Lattice encoding and decoding
  - Problems of shaping; LDLC decoding; Construction A decoding
- Lattices in multi-user networks: Compute and forward

What is a lattice?

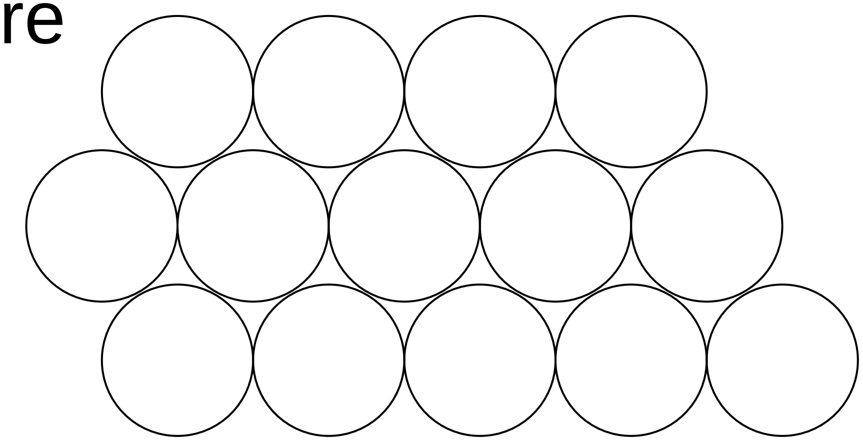
- A **lattice** is defined as:
  - the (infinite) set of points in an *n*-dimensional space given by all linear combinations with integer coefficients of a **basis** set of up to *n* linearly independent vectors
- It can be defined in terms of a **generator matrix G**, whose columns are the basis vectors:

$$\Lambda = \left\{ \lambda = \mathbf{G}\,\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n \right\}$$



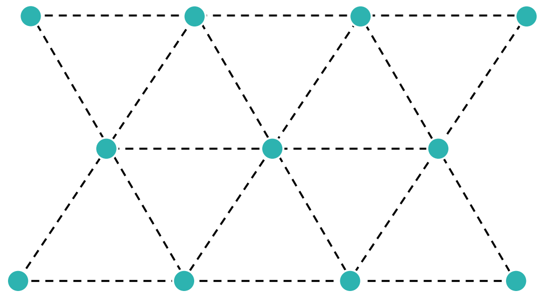
Sphere packings

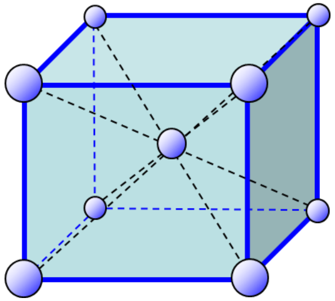
- A ***sphere packing*** is an arrangement of non-overlapping ***hyperspheres*** of equal radius in *N*-dimensional space
- We are often interested in the ***packing density*** η or δ_n of a packing
  - the proportion of space occupied by spheres
- Dense sphere packings are often ***lattice packings***
  - have sphere centres on lattices



Some lattices

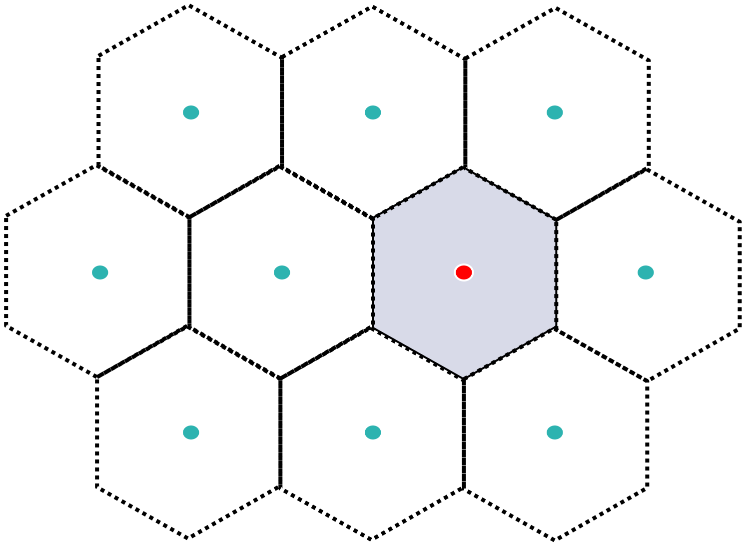
Dimensions	Lattice	Packing density	Kissing number
2	Hexagonal	$\frac{1}{6}\pi\sqrt{3}$=0.91	6
3	BCC/FCC/HCP	$\frac{1}{6}\pi\sqrt{2}$=0.74	12
4	D4	$\frac{1}{16}\pi^2 = 0.62$	24
8	E8	$\frac{1}{384}\pi^4 = 0.25$	240
24	E24 (Leech)	$\frac{\pi^{12}}{12!} = 0.0019$	196 560





Voronoi region

- The **Voronoi region** of a lattice point is the region of the *N*-dimensional space closer to that point than to all other lattice points
- Voronoi region of red point shown shaded



Outline

- Introduction to lattices
- **Codes and lattice codes**
  - **Shaping region**
  - **Nested lattices**
- Lattice constructions
- Lattice encoding and decoding
- Lattices in multi-user networks: Compute and forward

Codes

- i.e. ***forward error-correcting*** (FEC) codes
- A ***code*** is a finite set of ***codewords*** of length n
  - Code contains M codewords – encodes $\log_2(M)$ bits
- where a codeword is a sequence of n ***symbols***, usually drawn from a finite ***alphabet*** of size q
  - we will often assume the alphabet is a Galois field ($\mathbb{F}_q$ or GF(q)) or a ring ($\mathcal{R}(q)$)
- In a communication system the codewords must be translated into ***signals*** of length nT
  - representing the variation in time of some quantity, such as electromagnetic field strength
- Each code symbol is typically ***modulated*** to some specific real or complex value of this variable

Example

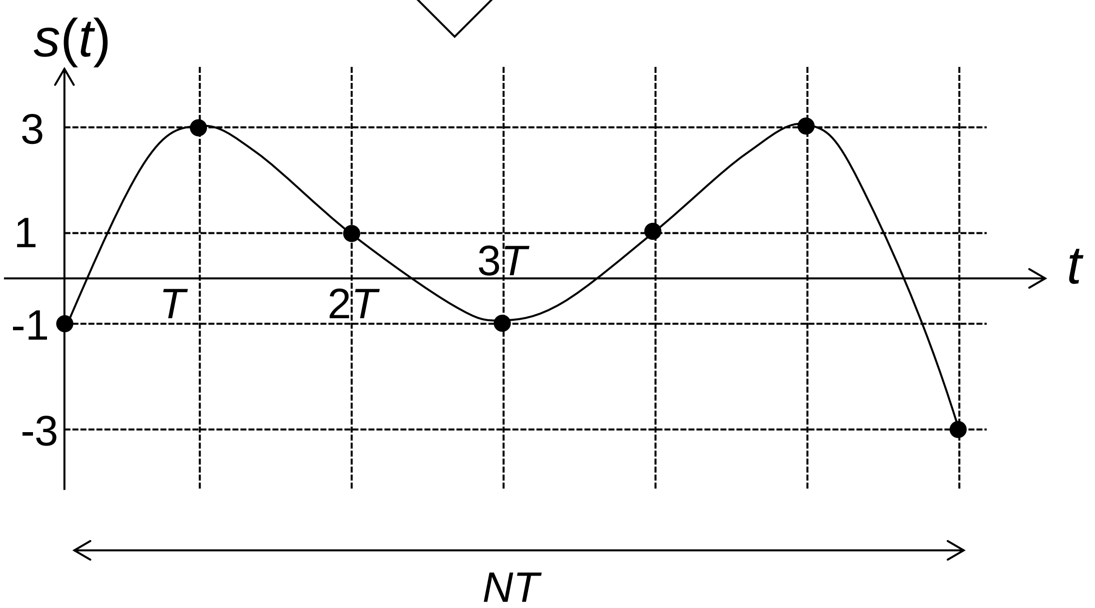
Message: 01111001

Encode

Codeword: 13212302

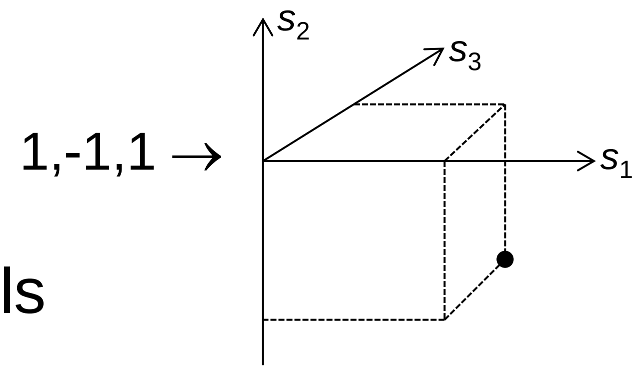
Modulate

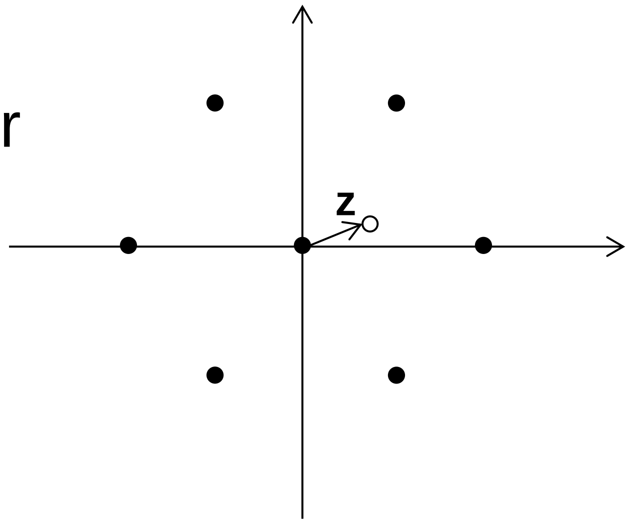
Signal:



Geometric model

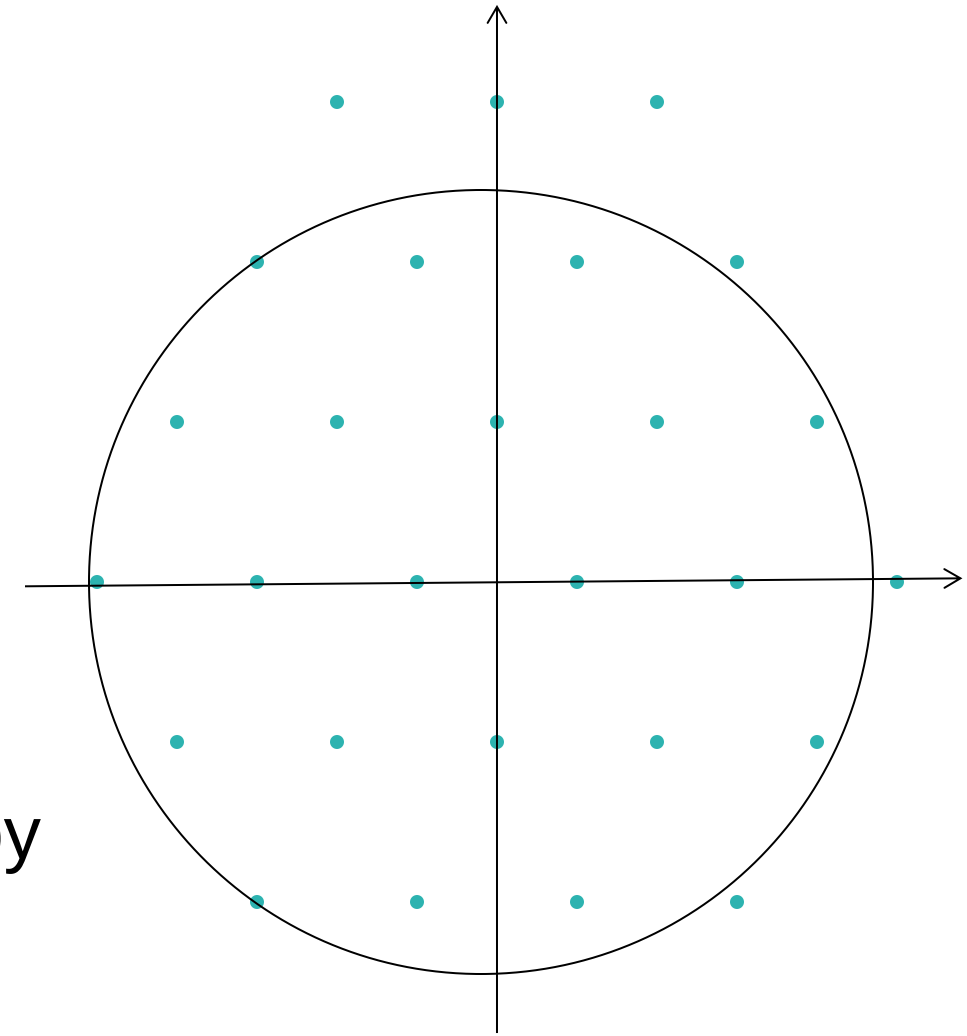
- Each coded signal can then be represented as a point in *N*-D ***signal space***
  - where modulated values of symbols provide the *n* coordinate values
- Code is represented by ensemble of points in signal space
- Noise on channel equivalent to vector z in signal space
- Decoder chooses closest point
- Error probability determined by ***minimum Euclidean distance*** between signal space points





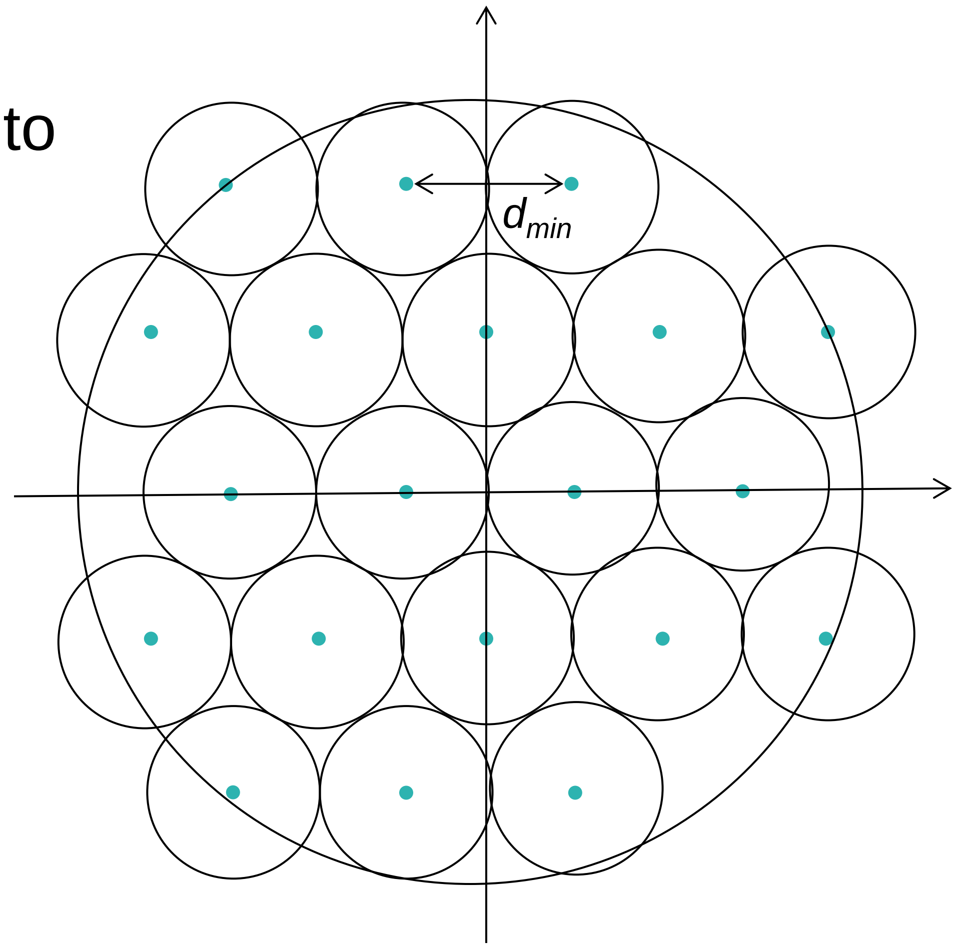
Lattice code

- A **lattice code** is then defined by the (finite) set of lattice points within a certain region
  - the **shaping region**
  - ideally a hypersphere centred on the origin
  - this limits the maximum signal energy of the codewords
- Lattice may be offset by adding some vector



Minimum Euclidean distance

- If the lattice is viewed as a sphere packing, then the minimum Euclidean distance must be twice the sphere radius
- Signal power S proportional to radius^2 of shaping region
- The greater the packing density, the greater M for given signal power
- Radius^2 of packed spheres proportional to maximum noise power

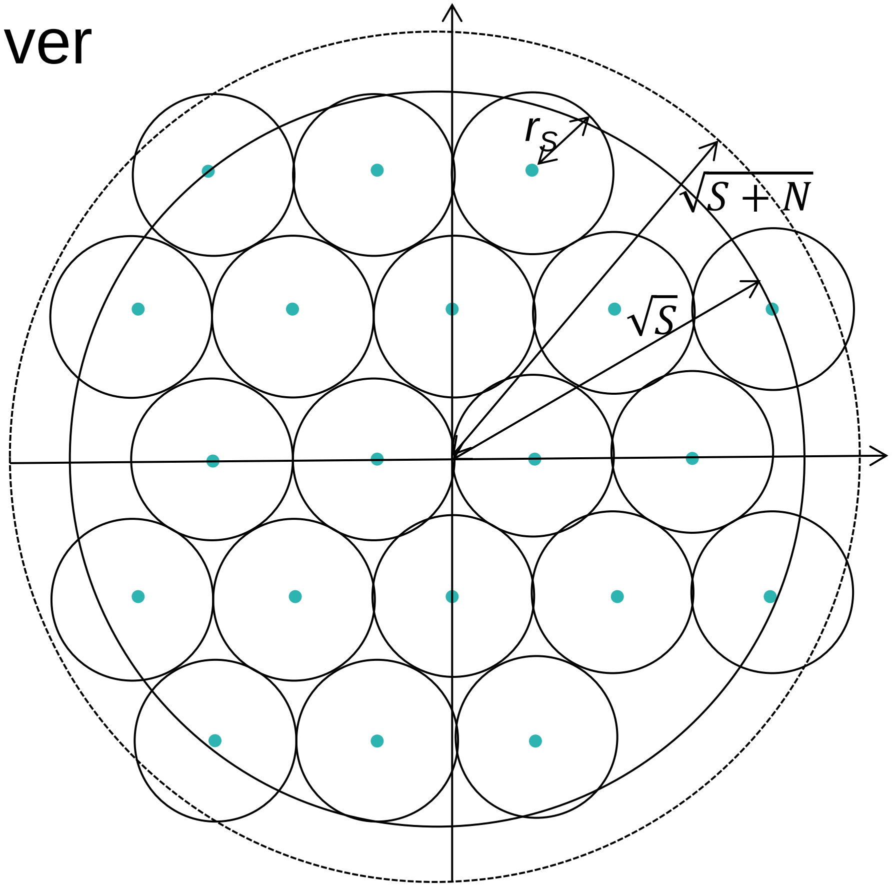


Maximum signalling rate

- Hence for low error probability, noise power $N \leq {r_S}^2$
- Radius of signal space at receiver containing signal plus noise is $\sqrt{S+N}$
- Volume of n-D sphere of radius r is $V_n r^n$
- Hence max. no. of codewords in code

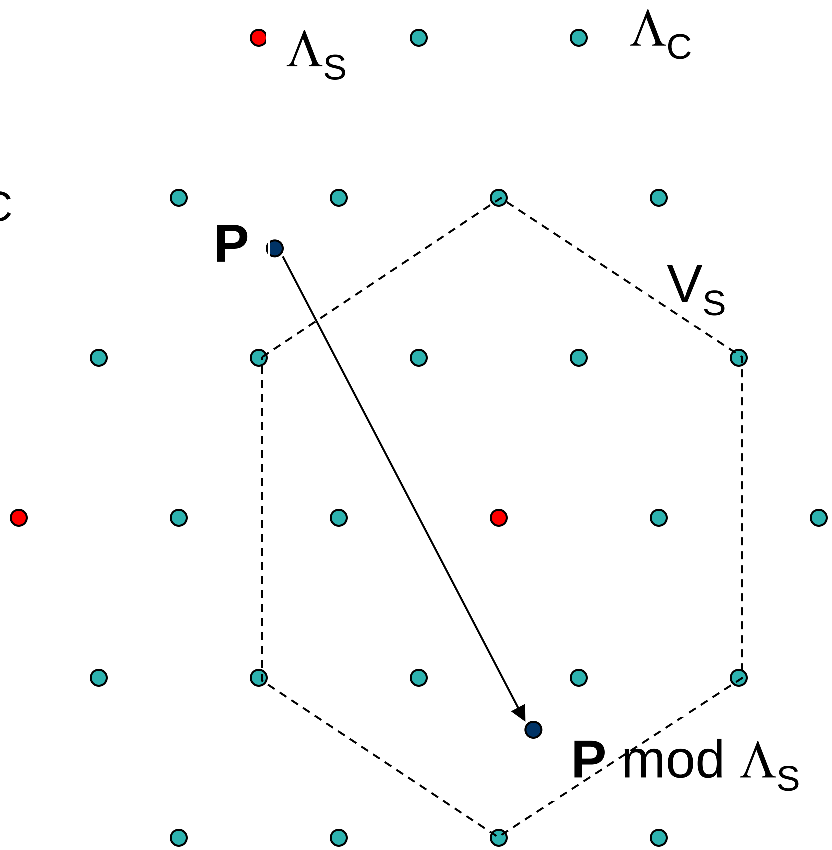
$$M \leq \frac{V_n (S+N)^{n/2}}{V_N {r_S}^{N/2}} \leq \left(\frac{S+N}{N}\right)^{n/2}$$

$$\frac{log_2 M}{n} \leq \frac{1}{2} log_2 \left(1 + \frac{S}{N}\right)$$



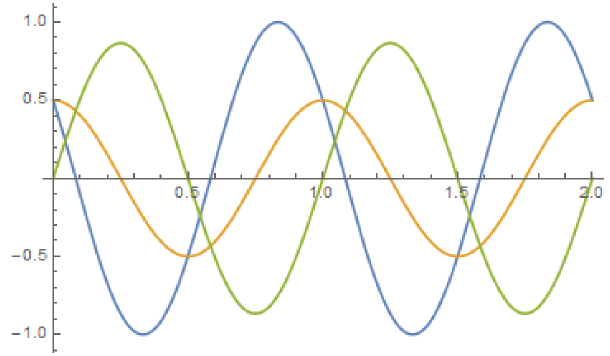
Nested lattice code

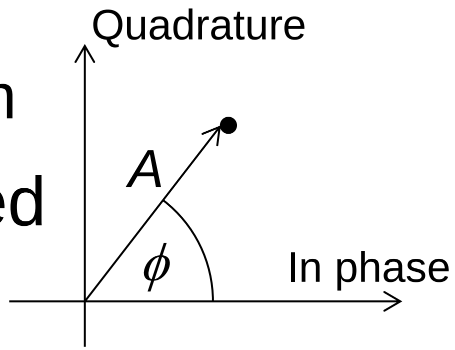
- Define fine lattice Λ_C for the code
  - plus a ***coarse lattice*** Λ_S which is a sub-lattice of Λ_C
- Then use a Voronoi region V_S of the coarse lattice as the shaping region
- Modulo-Λ_S operation
  - for any point $\mathbf{P} \notin V_S$ find $\mathbf{P} - (\lambda \in \Lambda_S) \in V_S$



Complex signals

- Wireless signals consist of a sine wave ***carrier*** at the transmission frequency (MHz – GHz)
- Sine waves can be modulated in both amplitude and phase
  - hence the signal corresponding to each modulated symbol is 2-D
  - also conveniently represented as a complex value
  - typically represented on a ***phasor*** diagram
- Hence wireless signals can be represented in 2n dimensions
  - or n complex dimensions





Outline

- Introduction to lattices
- Codes and lattice codes
- **Lattice constructions**
  - **Constructions A and D,**
  - **LDLC codes**
  - **Construction from Gaussian and Eisenstein integers**
- Lattice encoding and decoding
- Lattices in multi-user networks: Compute and forward

THE UNIVERSITY of York

Constructions based on FEC codes

- For practical purposes in communications, we require lattices in very large numbers of dimensions
  - typically 1000, 10 000, 100 000…
- Lattices of this sort of dimension most easily constructed using FEC codes such as LDPC and turbocodes
- Most common constructions encountered are called Constructions A and D (Conway and Sloane)
  - Construction A based on a single code
  - Construction D is multilevel, based on a nested sequence of codes

Construction A

- Start with a q-ary linear code $\mathcal{C}$ with generator matrix $\mathbf{G}_C$
- The set of vectors λ such that $\lambda \bmod q$ is a codeword of $\mathcal{C}$ form a Construction A lattice from $\mathcal{C}$:

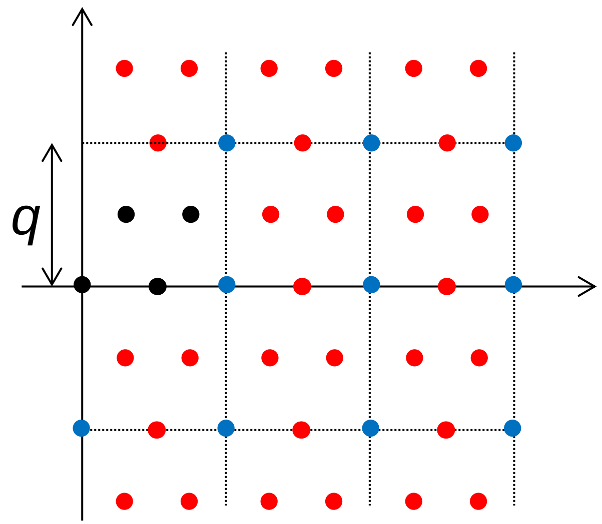
$$\Lambda = \left\{ \lambda : \lambda \bmod_q \in \mathcal{C} \right\}$$

- Alternatively we can write:

$$\Lambda = q\mathbb{Z}^n + \mathcal{C}$$

- The generator matrix of the lattice:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_C & \begin{matrix} \mathbf{0} \\ q\mathbf{I}_{n-k} \end{matrix} \end{bmatrix}$$



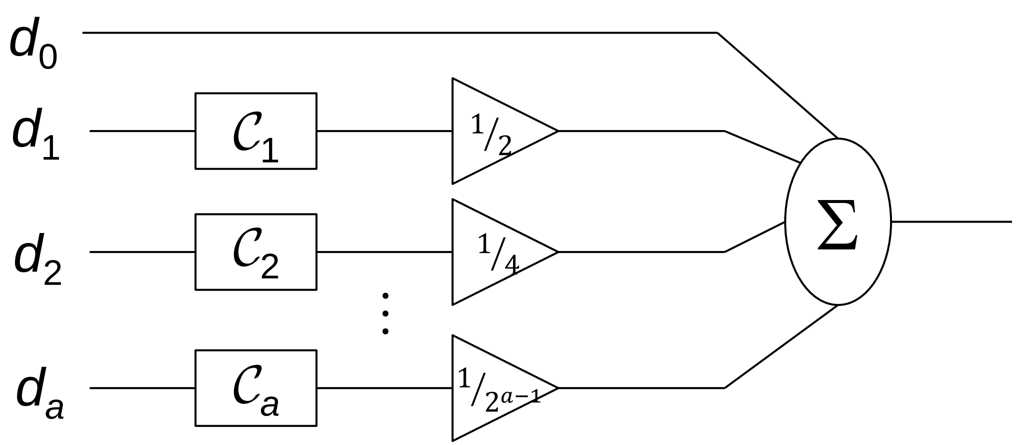
- Note that minimum distance is limited by q

Construction D

- Let $\mathcal{C}_0 \subseteq \mathcal{C}_1 \subseteq \mathcal{C}_2 \ldots \subseteq \mathcal{C}_a$ be a family of linear binary codes
  - where $\mathcal{C}_0$ is the (n, n) code and $\mathcal{C}_\ell$ is an (n, k_ℓ) code
- Then the lattice is defined by:

$$\Lambda = \left\{ \lambda : \lambda = \mathbf{z} + \sum_{l=1}^{a} \sum_{j=1}^{k_l} d_j^l \frac{\mathbf{c}_{j,l}}{2^{l-1}} \right\}$$

- where $\mathbf{z} \in 2\mathbb{Z}^n$, $\mathbf{c}_{j,\ell}$ is the j^{th} basis codeword of $\mathcal{C}_\ell$, and $d_j^\ell \in \{0,1\}$ denotes the j^{th} data bit for the ℓ^{th} code



Low density lattice codes

- Uses the principle of LDPC codes:
  - Define generator matrix such that its inverse $\mathbf{H} = \mathbf{G}^{-1}$ is sparse
  - Then decode using sum-product algorithm (message passing) as in LDPC decoder
- However elements of **H** and **G** are reals (or complex) rather than binary
  - Messages are no longer simple log-likelihood ratios
- Ideally use nested lattice code
  - i.e. shaping region is Voronoi region of a coarse lattice

THE UNIVERSITY of York

Gaussian and Eisenstein integers

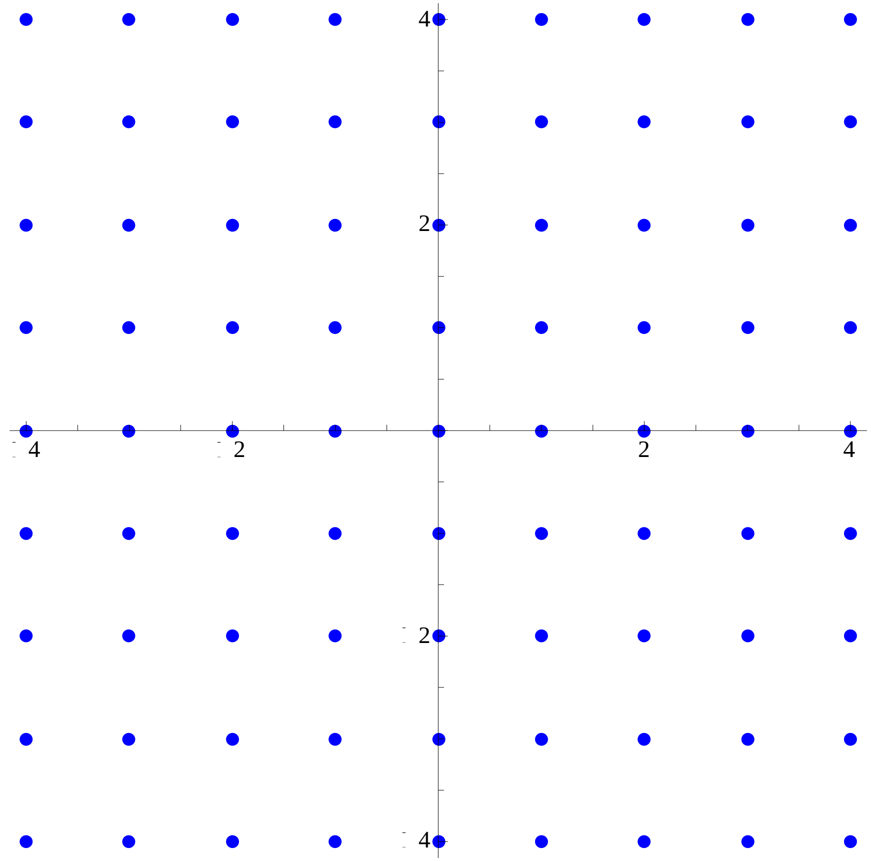
- Construction A/D and LDLC result in real lattices
  - can exploit Gaussian/Eisenstein integers to construct complex lattices
- Gaussian and Eisenstein integers form the algebraic equivalent in complex domain of the ring of integers
- Can construct complex constellations from them which form complex lattices

Gaussian Integers

- Gaussian integers are the set of complex numbers with integer real and imaginary parts, denoted

$$\mathbb{Z}[\mathrm{i}] = a + b\mathrm{i},\ a, b \in \mathbb{Z}$$

- They form a ring on ordinary complex arithmetic
- Hence operations in the ring exactly mirror operations in signal space
- Also form a lattice



Nested lattice of Gaussian integers

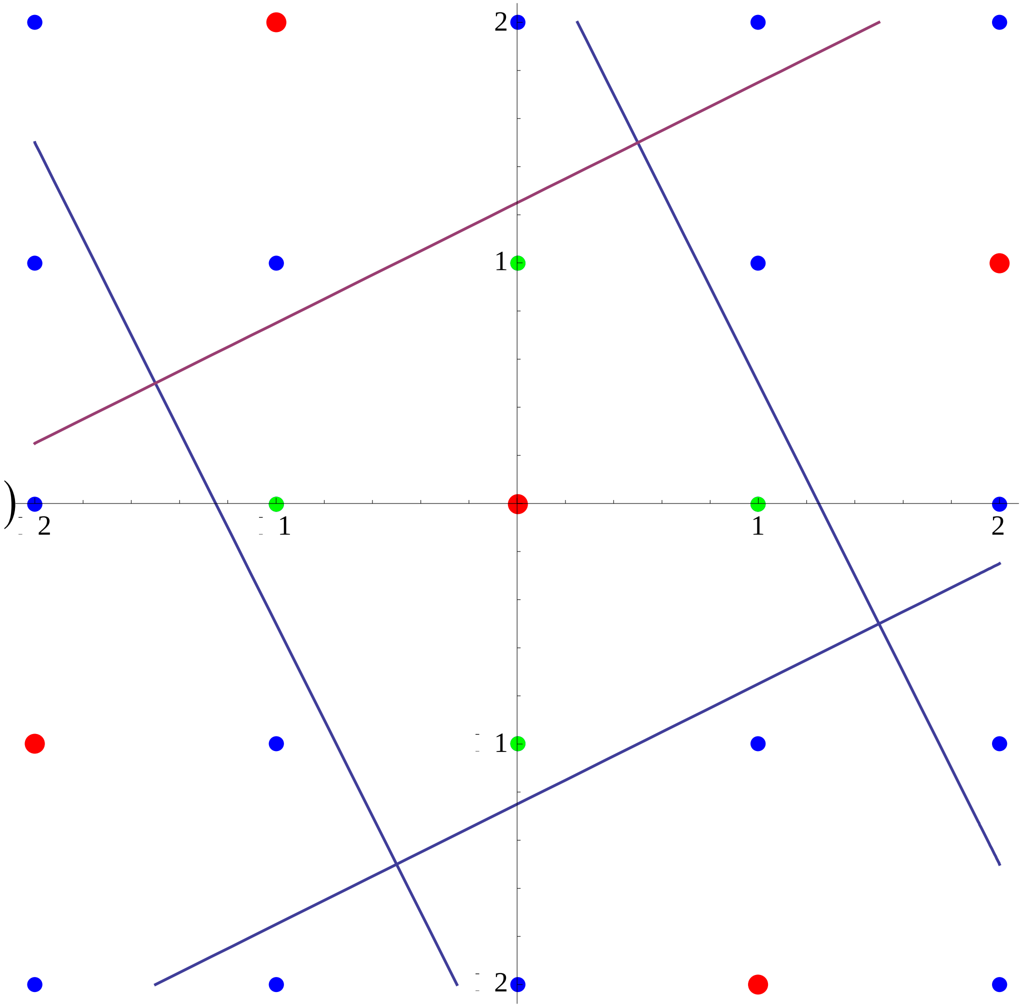
- Consider *fine* and *coarse* lattices, Λ_f and Λ_c, both based on Gaussian integers

$$\Lambda_c \subset \Lambda_f$$

- Here we assume that each point in the coarse lattice is a point in the fine multiplied by some Gaussian integer *q*
  - i.e. the coarse is a scaled and rotated version of the fine
  - and the fine is just the Gaussian integers
- We then define our constellation as consisting of those Gaussian integers which fall in the Voronoi region of the coarse lattice

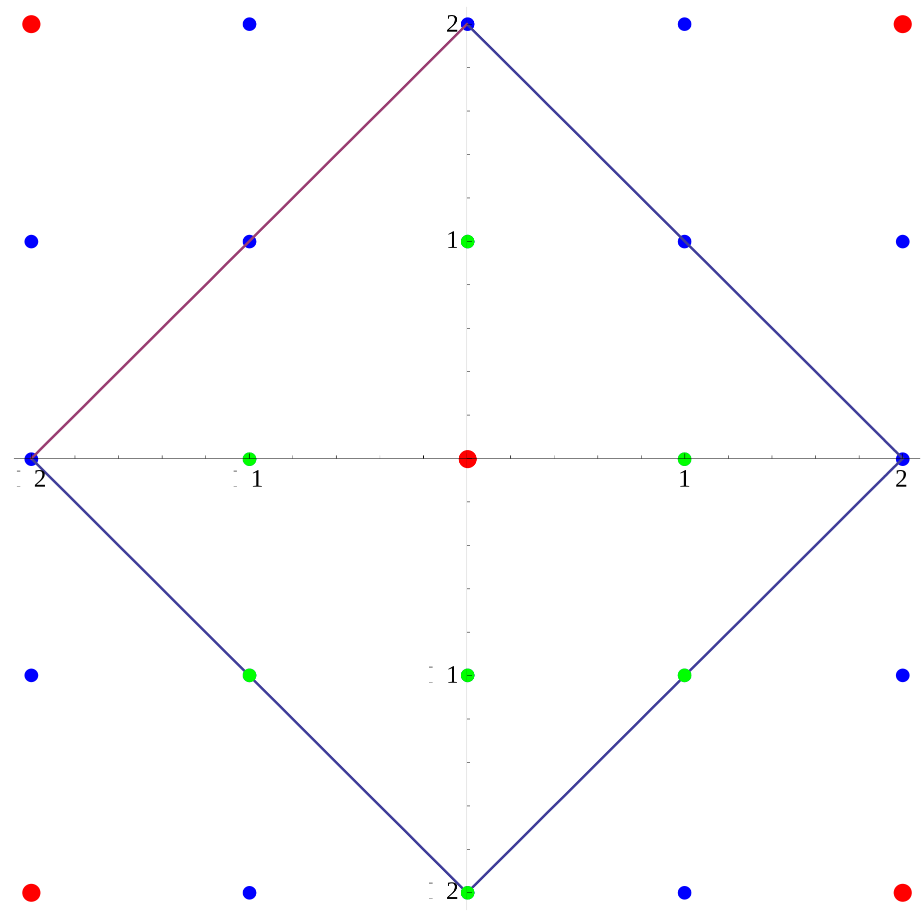
Example

- e.g. $q = 2 + i$
- Blue points are fine lattice
- Red points are coarse lattice
- Fundamental region $V_c(0)$ is region closer to origin than any other coarse lattice point
- Hence constellation is green points, inc origin



Boundary points

- The fundamental region is surrounded by regions corresponding to $q, qi, -q$ and $-qi$
- We treat the boundaries of the latter two as belonging to the fundamental region
  - use this to allocate certain boundary points to constellation
- This also leads to an alternative definition of the fundamental region:



$$V_c(0) = \left\{ \lambda \in \mathbb{C} : \left(-\frac{|q|^2}{2} \le \Re[\lambda]\Re[q] + \Im[\lambda]\Im[q] < \frac{|q|^2}{2} \right) \;\&\; \left(-\frac{|q|^2}{2} \le -\Re[\lambda]\Im[q] + \Im[\lambda]\Re[q] < \frac{|q|^2}{2} \right) \right\}$$

Isomorphisms

- We can establish ***isomorphisms*** between these constellations and either fields or rings
- An isomorphism is a one-to-one (or *bijective*, and hence invertible) mapping between the constellation $\mathcal{C}$ and the ring $\mathcal{R}$ $\lambda = \mathcal{M}(s), \lambda \in \mathcal{C}, s \in \mathcal{R}$ $s = \mathcal{M}^{-1}(\lambda), \lambda \in \mathcal{C}, s \in \mathcal{R}$
- such that the operations on the ring are equivalent to those on the constellation

$$\mathcal{M}(s_1 \otimes s_2) = \mathcal{M}(s_1)\mathcal{M}(s_2) \quad \mathcal{M}(s_1 \oplus s_2) = \mathcal{M}(s_1) + \mathcal{M}(s_2)$$

- It turns out that if *q* is a ***Gaussian prime***, then the constellation is isomorphic to a field, otherwise it is isomorphic to a ring
- Size of field/ring is $|q|^2$

Lattice construction

- This isomorphism can be used to construct a complex lattice from a code based on the field or ring
  - in a manner equivalent to Construction A

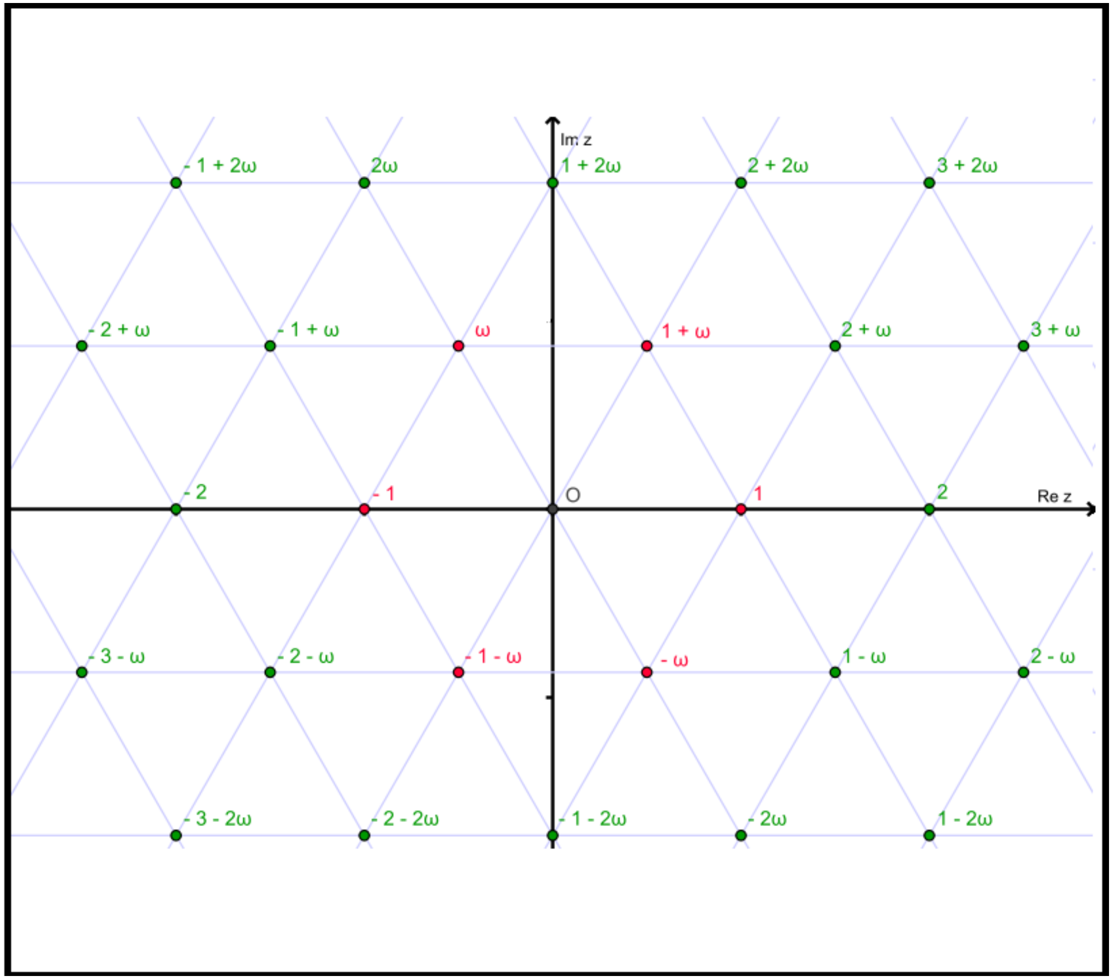
$$\Lambda = \left\{ \lambda : \lambda = \mathbf{z} + \mathcal{M}(\mathbf{c}), \mathbf{z} \in q\mathbb{Z}[i]^n, \mathbf{c} \in \mathcal{C}\left(\mathbb{F}_{|q|^2}\right) \right\}$$

  - that is, we encode a data sequence in the field $\mathbb{F}_q$ using the code $\mathcal{C}$ (over $\mathbb{F}_{|q|^2}$)
  - then map the resulting symbols to the complex constellation using the mapping based on the isomorphism
  - then combine with a lattice of Gaussian integers scaled by q

Eisenstein integers

- Set of complex values with similar properties to Gaussian integers
- Hexagonal structure may result in denser lattices
- Note:

$$\omega = \frac{1 + i\sqrt{3}}{2} = e^{2\pi i/3}$$

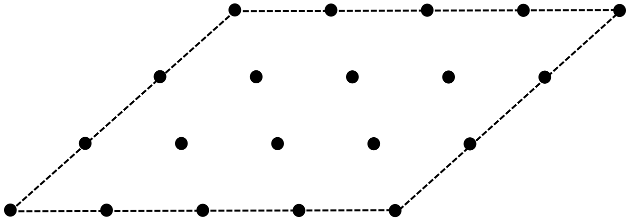


Outline

- Introduction to lattices
- Codes and lattice codes
- Lattice constructions
- **Lattice encoding and decoding**
  - **Problems of shaping**
  - **Construction A/D decoding**
  - **LDLC decoding**
- Lattices in multi-user networks: Compute and forward

Shaping

- Ideally the shaping region should be as close as possible to a hypersphere
  - provides ***shaping gain*** up to 1.5 dB compared to hypercube shaping
- Nested lattice shaping gives a good approximation to this
- First multiply data vector by generator matrix
  - this may generate region of lattice of arbitrary shape
- Then apply modulo-lattice operation:
  - decode to coarse lattice, and subtract resulting coarse lattice vector



- In practice this decoding operation may be difficult
  - may use hypercube shaping as simpler alternative

Construction A decoding

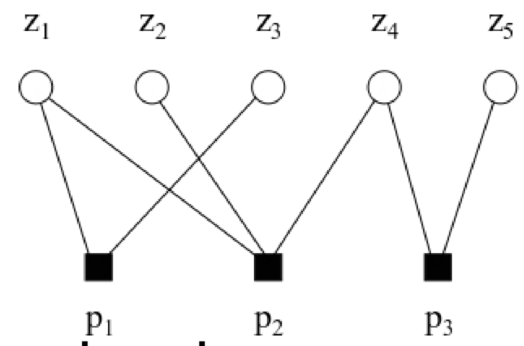
- Generally can be carried out with decoder for underlying code $\mathcal{C}$
- Applying mod_q operation regenerates codeword of $\mathcal{C}$
  - then decode this codeword
  - can then recover specific point in $\mathbb{Z}^n$
- Note that in practice we use non-binary codes ($q > 2$)
  - because $q = 2$ limits minimum distance and hence coding gain
- Typically use LDPC or turbocodes to achieve good performance
  - hence need non-binary sum-product or BCJR decoder
  - messages are probability distribution of q symbol values

Construction D decoding

- Use multilevel decoding approach based on component codes
  - decode codes $\mathcal{C}_a$, $\mathcal{C}_{a\text{-}1}$, … $\mathcal{C}_1$ in succession
- Component codes may usually be binary
- May require iterative approach
  - c.f. multilevel coded modulation

LDLC decoding

- Code structure designed for sum-product decoding, cf LDPC
  - using ***factor graph***



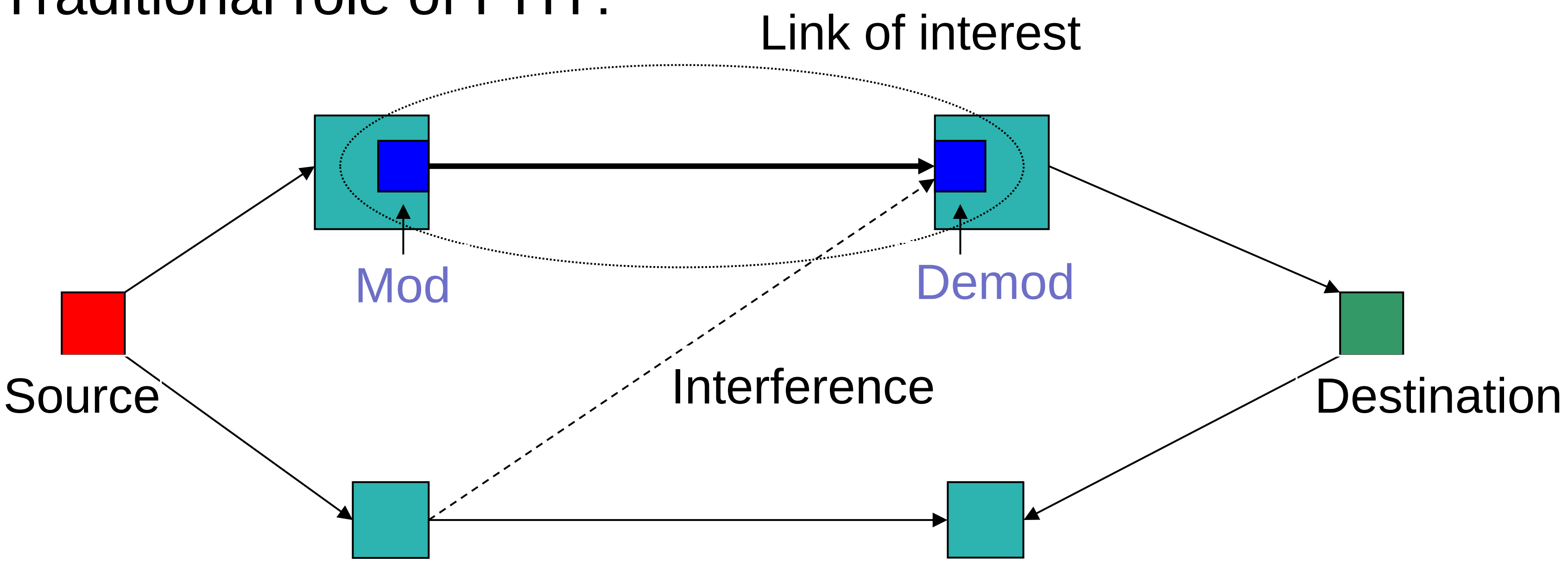
- However symbol values are now continuous variables (reals)
  - hence messages should be probability density functions
  - requires compact means of representing PDF in decoder
- May use Fourier or Karhunen-Loeve basis representation
  - or Gaussian mixture model

Outline

- Introduction to lattices
- Codes and lattice codes
- Lattice constructions
- Lattice encoding and decoding
- **Lattices in multi-user networks**
  - **Wireless physical-layer network coding**
  - **Compute and forward**

Physical layer in multi-user networks

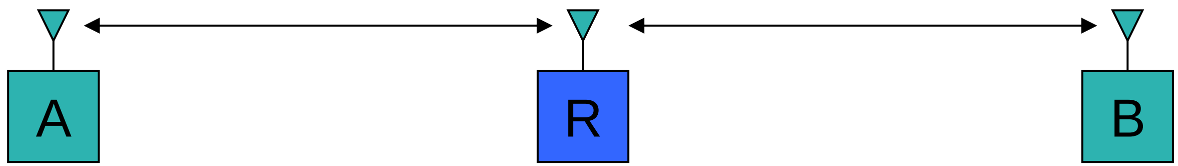
- Traditional role of PHY:



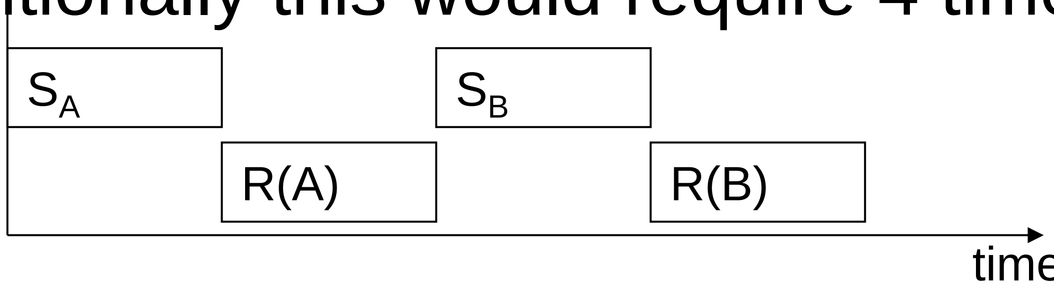
- signals from elsewhere in network treated as harmful interference
- however they may carry related information that can be exploited

Two-way relay channel

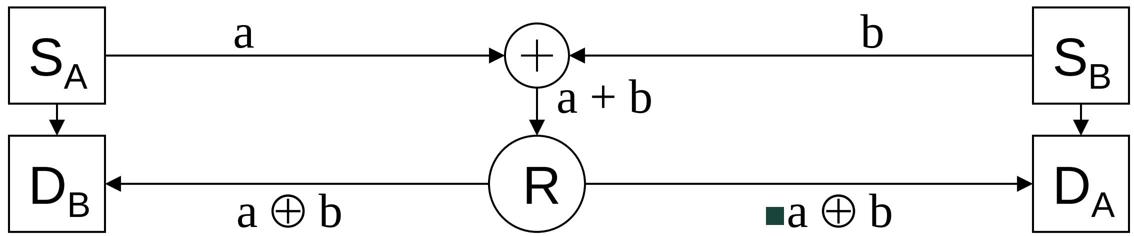
- Two terminals want to exchange data via a relay:



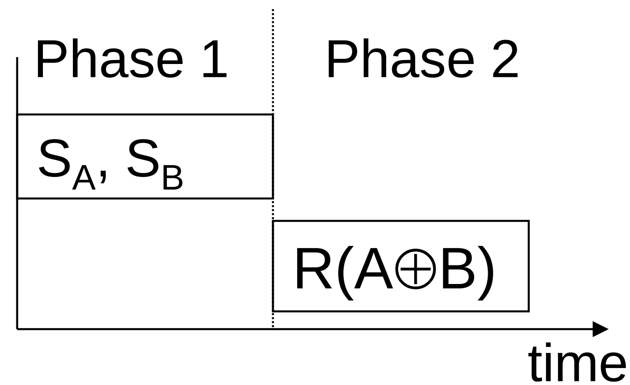
- Conventionally this would require 4 time-slots:



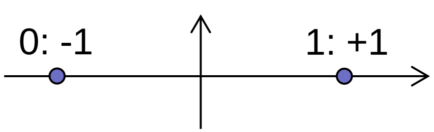
WPNC

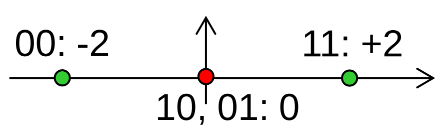


- We can do better using *Wireless Physical-layer Network Coding*
  - using two phases
- Assume both sources transmit BPSK:
  - map data symbol ‘1’ to signal +1; ‘0’ to -1
- At relay, map signals +2 and -2 to ‘0’; 0 to ‘1’



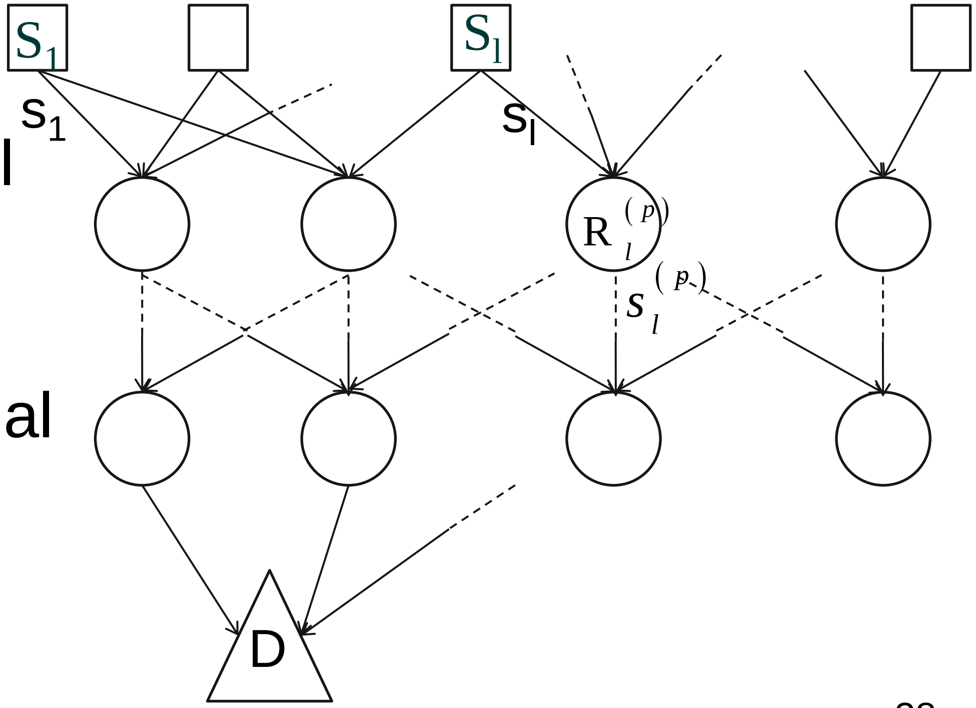
a	b	a+b	a ⊕ b
0	0	-2	0
0	1	0	1
1	0	0	1
1	1	+2	0





A general network model

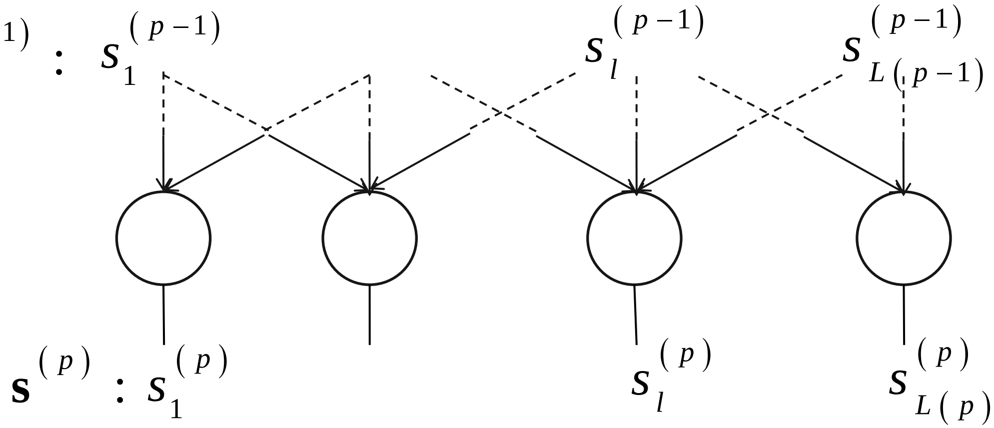
- Model a network with *P* layers of relays
- In general all nodes in a layer transmit simultaneously
- Each relay decodes a (linear) function of symbols from previous layer $s_l^{(p)} = a_{1l} s_1^{(p-1)} + a_{2l} s_2^{(p-1)} + \cdots a_{Ll} s_L^{(p-1)} = \mathbf{a}_l . \mathbf{s}^{(p-1)}$
- based on the combined signals they receive
- Destination extracts symbol it is interested in from outputs of functions
- Lattices provide useful signal sets



Network coding model of network

- We can relate the vector of outputs of each layer to its inputs via the matrix **A:**

$$\mathbf{s}^{(p)} = \mathbf{A}^{(p)}\mathbf{s}^{(p-1)}$$



- We can combine these in cascade, so that:

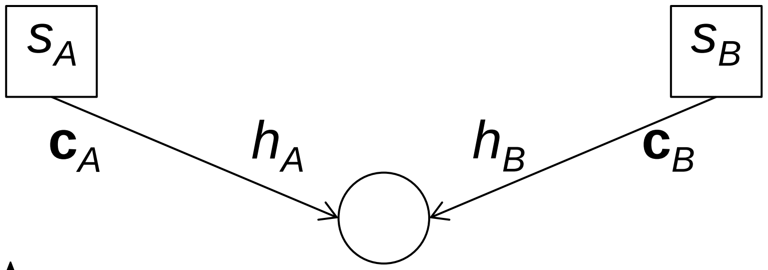
$$\mathbf{s}^{(p)} = \mathbf{A}^{(p)}\mathbf{A}^{(p-1)}\cdots\mathbf{A}^{(1)}\mathbf{s}$$

- We can write this as a single matrix relating the vector of symbol $\mathbf{s}^D$ at relays connected to the destination:

$$\mathbf{s}^D = \mathbf{B}\,\mathbf{s}$$

- We assume that the destination can (in principle) decode all symbols in its connection set

Lattice signal sets



- Consider relay receiving from two sources via channel h_A, h_B
- Sources transmit codewords $\mathbf{c}_A$, $\mathbf{c}_B$ from the same fine lattice Λ_C
- Received signal at relay is then:

$$\mathbf{x} = h_A \mathbf{c}_A + h_B \mathbf{c}_B + \mathbf{w}$$

- Now the sum of any integer multiples of two lattice points is another lattice point
  - hence if h_A, h_B were integers we could decode at the relay using the same lattice decoder
- Key idea is to scale received signal by scaling factor α so that αh_A and αh_B are approximately integers

Optimum approximation

- Then:

$$\alpha\mathbf{x} = \alpha h_A \mathbf{c}_A + \alpha h_B \mathbf{c}_B + \alpha \mathbf{w} \approx a_A \mathbf{c}_A + a_B \mathbf{c}_B$$

  - where a_A and a_B are integers
- Approximation error is:

$$(\alpha h_A - a_A)\,\mathbf{c}_A + (\alpha h_B - a_B)\,\mathbf{c}_B + \alpha\mathbf{w}$$

- We can minimise this by choosing α:

$$\alpha_{\text{MMSE}} = \frac{P\sum_i h_i a_i}{N + P\sum_i |h_i|^2}$$

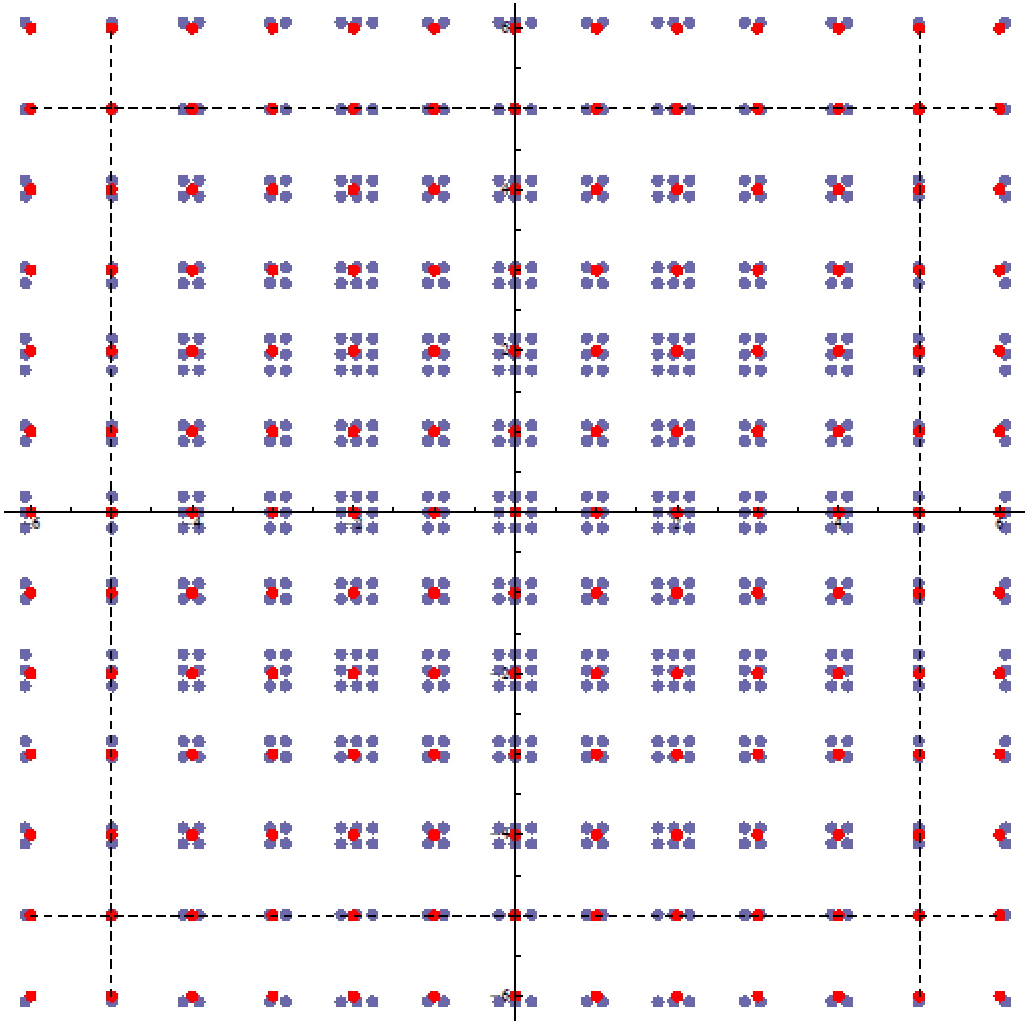
  - where P is signal power
- Also need to choose a_A and a_B
  - could choose such that $a_A/a_B = h_A/h_B$
  - but might require large α, and hence increase noise

Example

- $h_A = 0.55$; $h_B = 1.0$
- Choose:

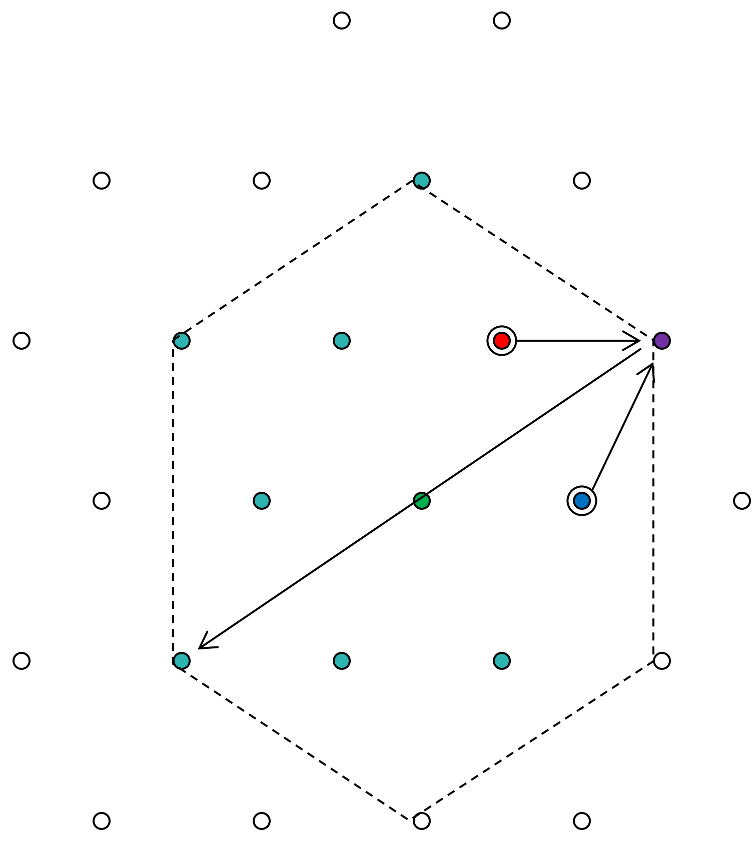
  $a_A = 1$; $a_B = 2$;
  $\alpha = 1.95$

- Blue points are received signal
- Red are approximated lattice



Modulo-Λ operation

- Sum of two points from a lattice code may in general result in point outside shaping region
- Hence we apply modulo-lattice operation
  - returns a point in the original lattice code
  - so we can use the same decoder to recover sum point
- For lattice constellations isomorphic with field this operation can always be inverted

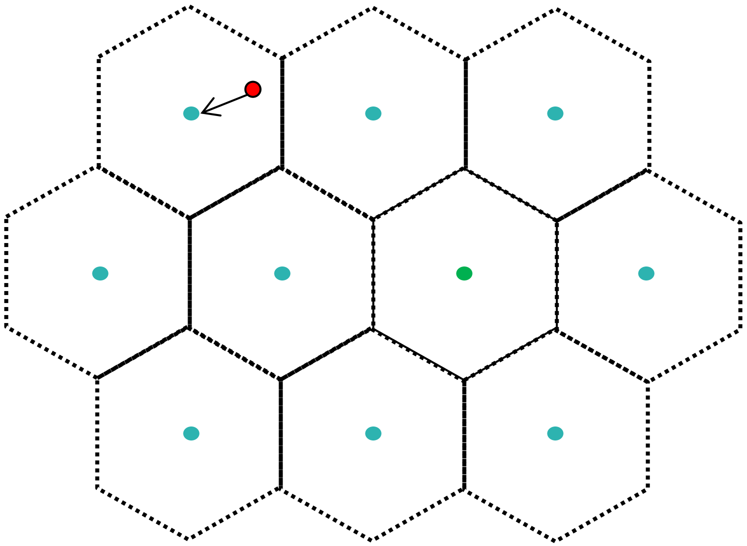


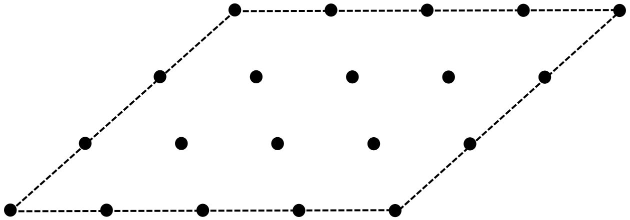
Conclusions

- Lattices can be extensively used in communications
  - especially for ***lattice coding***
- Can be shown to achieve capacity, as lattice dimension tends to infinity
- Practical lattice constructions are based on FEC codes
  - can provide high dimension lattices
  - with practical decoding algorithms
- For wireless channels use complex lattice constellations based on Gaussian/Eisenstein integers
- Important application is ***compute and forward***
  - applies to relay networks

More lattice applications

- Lattice quantisation:
  - quantising signals to lattice points in high dimension can reduce mean square error
  - Applying modulo-lattice operation also allows Wyner-Ziv compression of correlated sources
- Lattice reduction aided MIMO detection
  - MIMO channel may distort received signal:
  - LRA treats as a different lattice





Bibliography

- John Conway and Neil J. A. Sloane “Sphere Packings, Lattices and Groups”, Springer, 1999, ISBN 978-1-4757-6568-7
- Uri Erez, Shlomo Shamai (Shitz), and Ram Zamir “Achieving 1/2 log(1 + SNR) on the AWGN channel with lattice encoding and decoding”, *IEEE Trans. Inf. Theory, 50(10):2293–2314, October 2004.*
- Ram Zamir “Lattice Coding for Signals and Networks
  A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory” Cambridge University Press, 2014, ISBN: 9780521766982
- Naftali Sommer, Meir Feder, and Ofir Shalvi “Low-density lattice codes”, *IEEE Trans. Inf. Theory, 54(4):1561–1585, April 2008.*
- Bobak Nazer and Michael Gastpar “Compute-and-forward: Harnessing interference through structured codes”, *IEEE Trans. Inf. Theory, 57(10):6463–6486, Oct 2011.*