THE UNIVERSITY *of York*

Multilevel Lattice Network Codes

Alister Burr and Yi Wang,
University of York
alister.burr@york.ac.uk

Outline

- Introduction: Lattices in wireless communications
- Multilevel coded modulation
- Multilevel lattices: the *elementary divisor construction*
- Multilevel lattice decoding
  - Layered Integer Forcing
  - Iterative decoding
- Conclusions

THE UNIVERSITY *of York*

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 (□$_q$ or GF(q)) or a ring (□(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

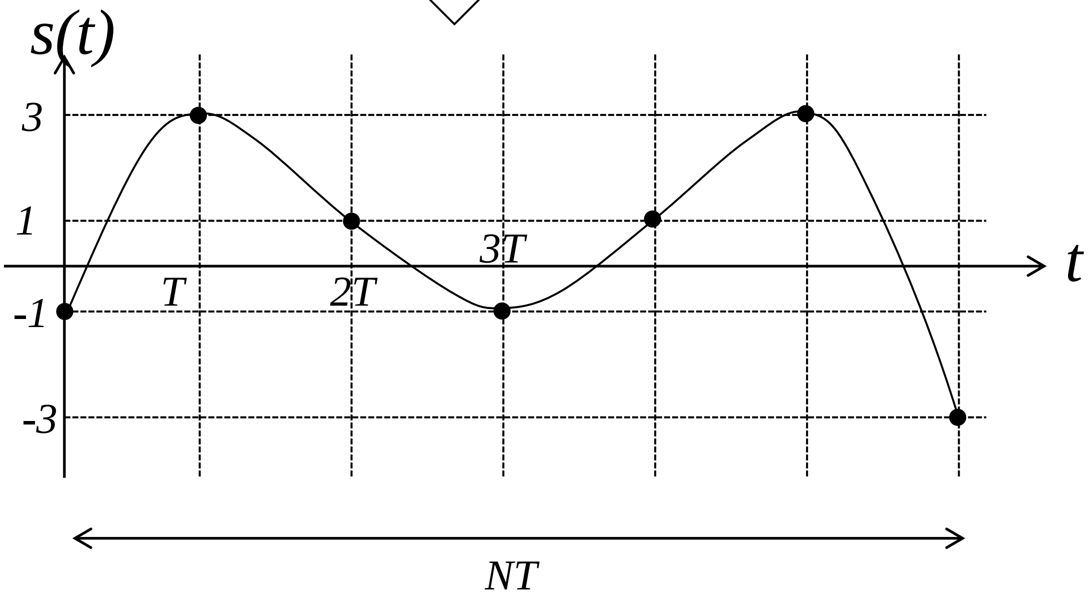
Message: *01111001*

Encode

Codeword: *1321230*

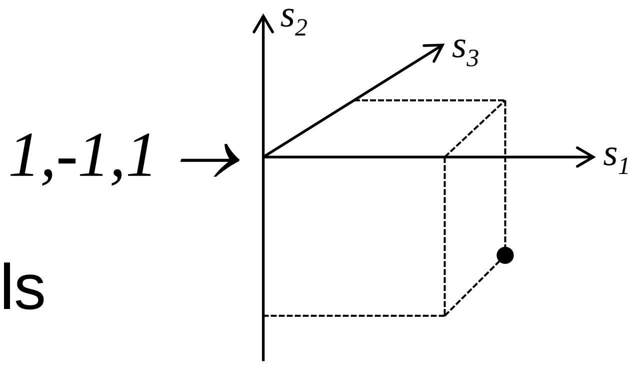
Modulate

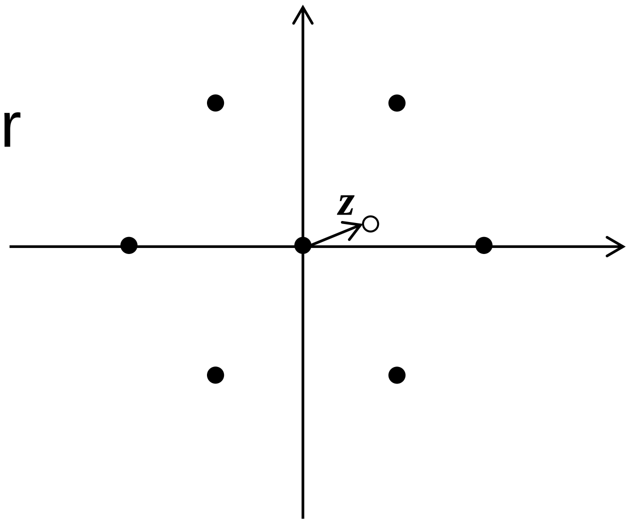
Signal:



Geometric model

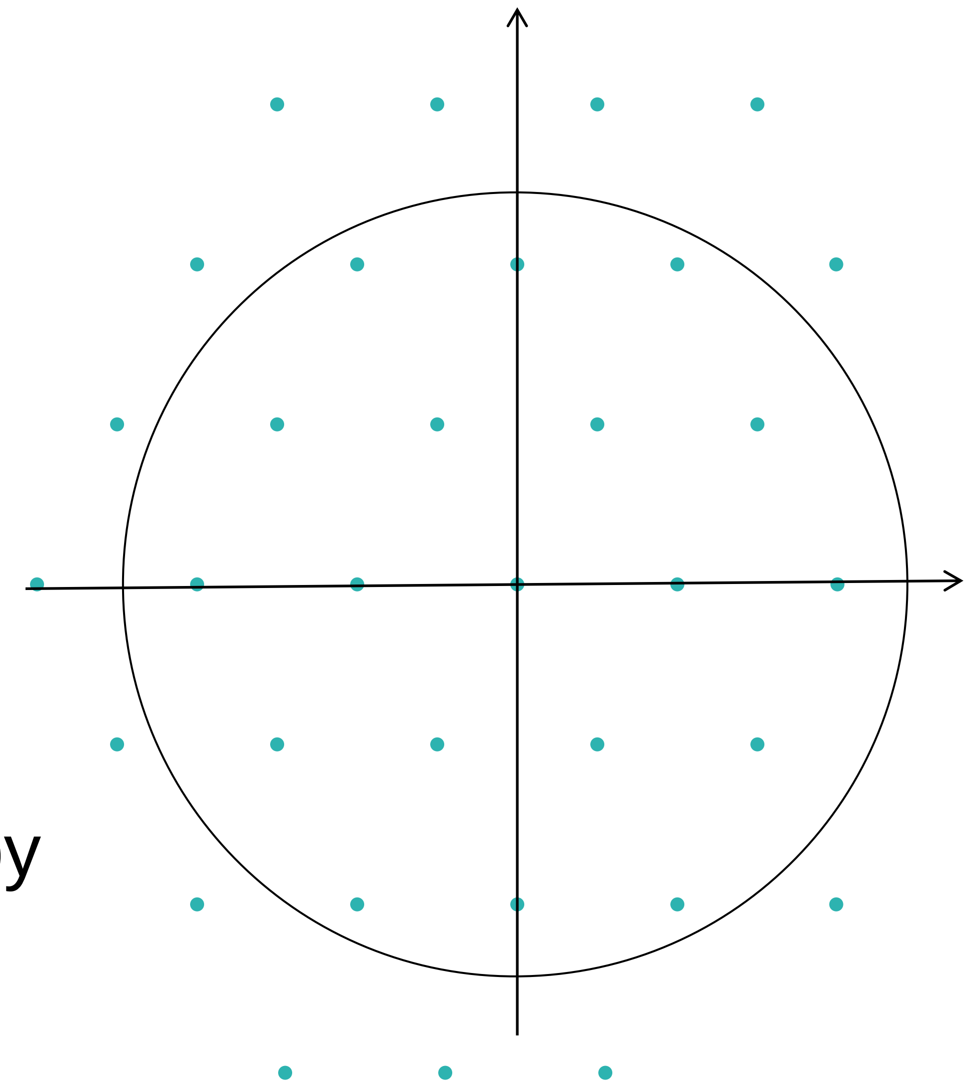
- Each coded signal can then be represented as a point in *N*-D ***signal space***
  - where modulated values of symbols provide the *n* coordinate values
- Code is represented by ensemble of points in signal space
- Noise on channel equivalent to vector z in signal space
- Decoder chooses closest point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





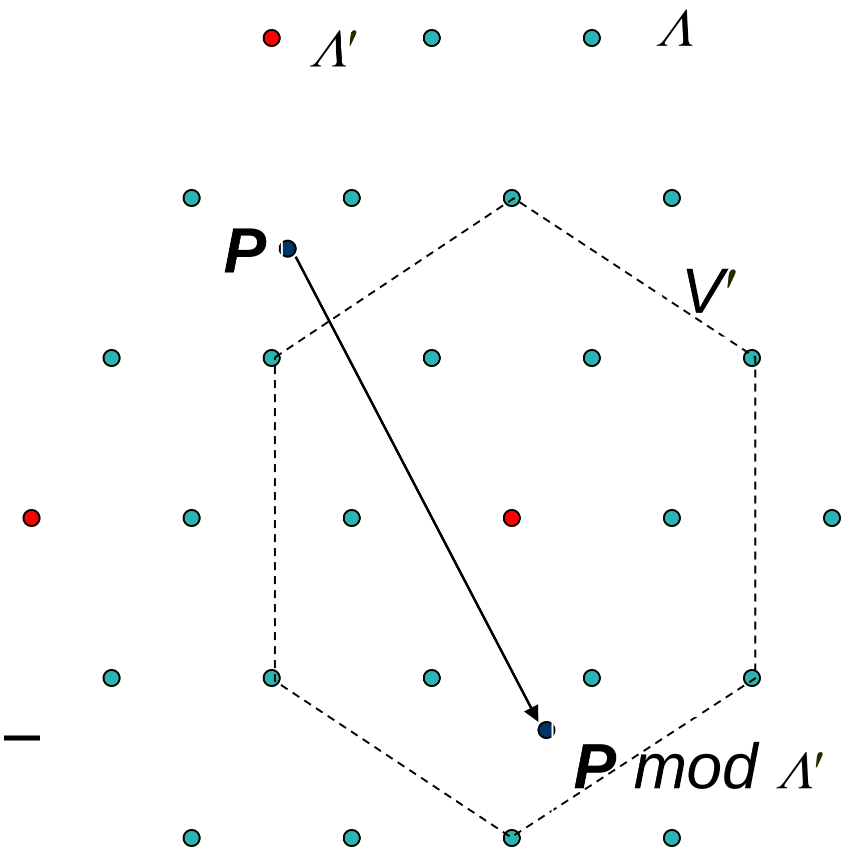
Lattice code

- 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



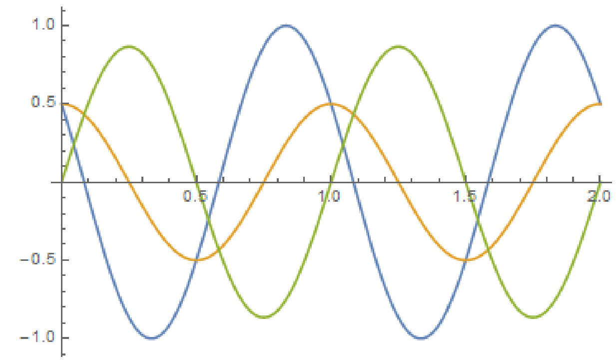
Nested lattice code

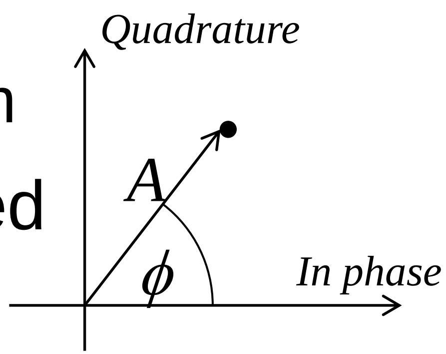
- Define fine lattice Λ for the code
  - plus a ***coarse lattice*** Λ' which is a sub-lattice of Λ
- Then use a Voronoi region V′ of the coarse lattice as the shaping region
- Modulo-Λ' operation
  - for any point **P** $\notin$ V′ find **P** – ($\lambda \in \Lambda'$) $\in$ V′



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 2*n* dimensions
  - or *n* complex dimensions





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 $\mathcal{C}$:

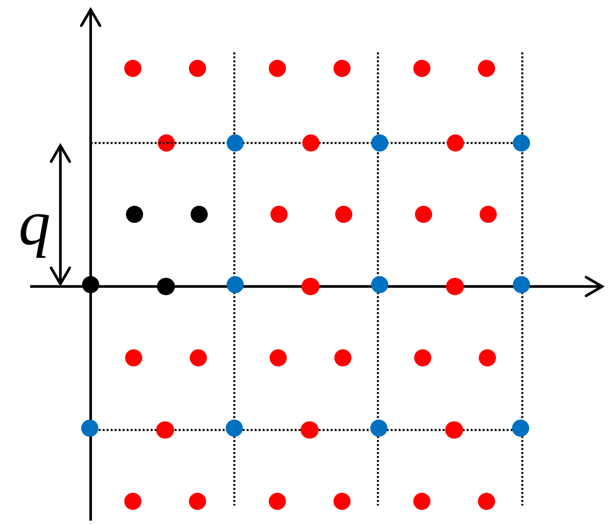
$$\Lambda = \{\lambda : \lambda \,\mathrm{mod}_q \in \mathrm{C}\}$$

- Alternatively we can write:

$$\Lambda = q\mathbf{Z}^n + \mathrm{C}$$

- The generator matrix of the lattice:

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



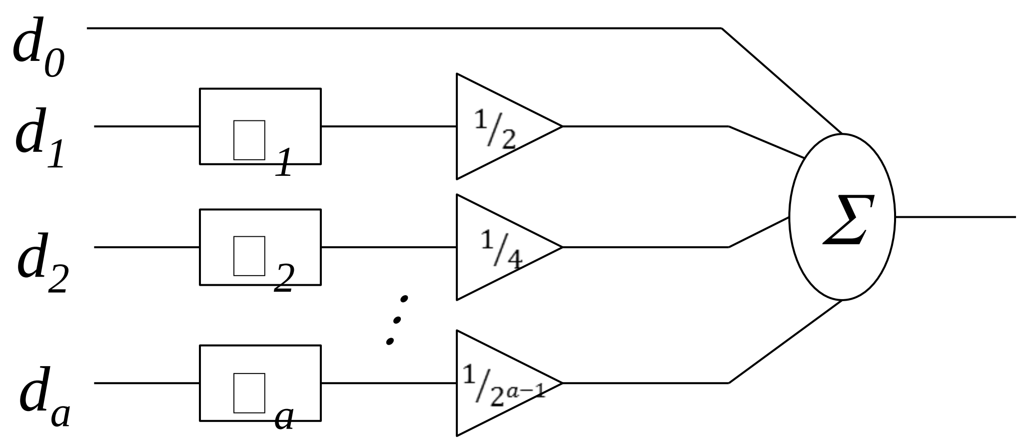
- Note that minimum distance is limited by q
  - this also limits the *coding gain* of the lattice code to at

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:

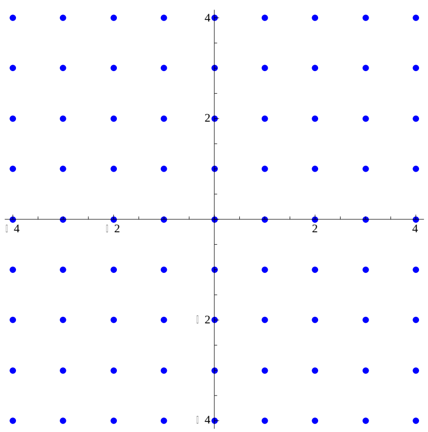
$$\Lambda = \left\{ \lambda : \lambda = \mathbf{z} + \sum_{l=1}^{a} \sum_{j=1}^{k_l} d_j^l \frac{\mathbf{c}_{j,l}}{2^{l-1}} \right\}$$

- 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

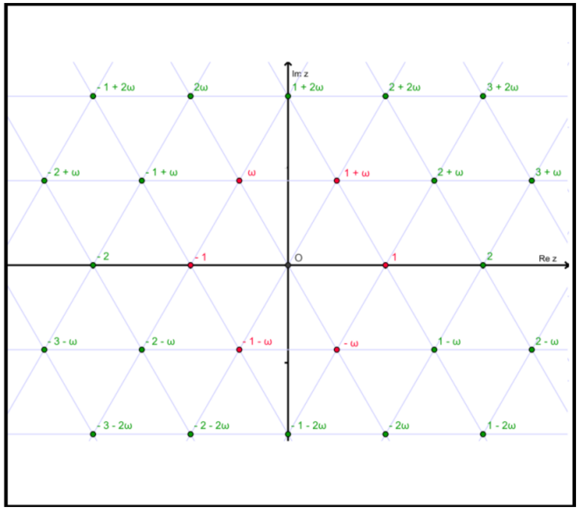


Construction of complex lattices

- Construction A/D as described result in real lattices, based on integers
- Gaussian and Eisenstein integers form the algebraic equivalent in complex domain of the ring of integers
  - all are Principal Ideal Domains (PID)
- Hence can similarly construct complex constellations from them to form complex lattices



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



$$\mathbb{Z}[\omega] = a + b\,\omega,\ a, b \in \mathbb{Z},\ \omega = e^{2\pi i/3}$$

Nested lattice of Gaussian integers

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

$$\Lambda_c \subset \Lambda$$

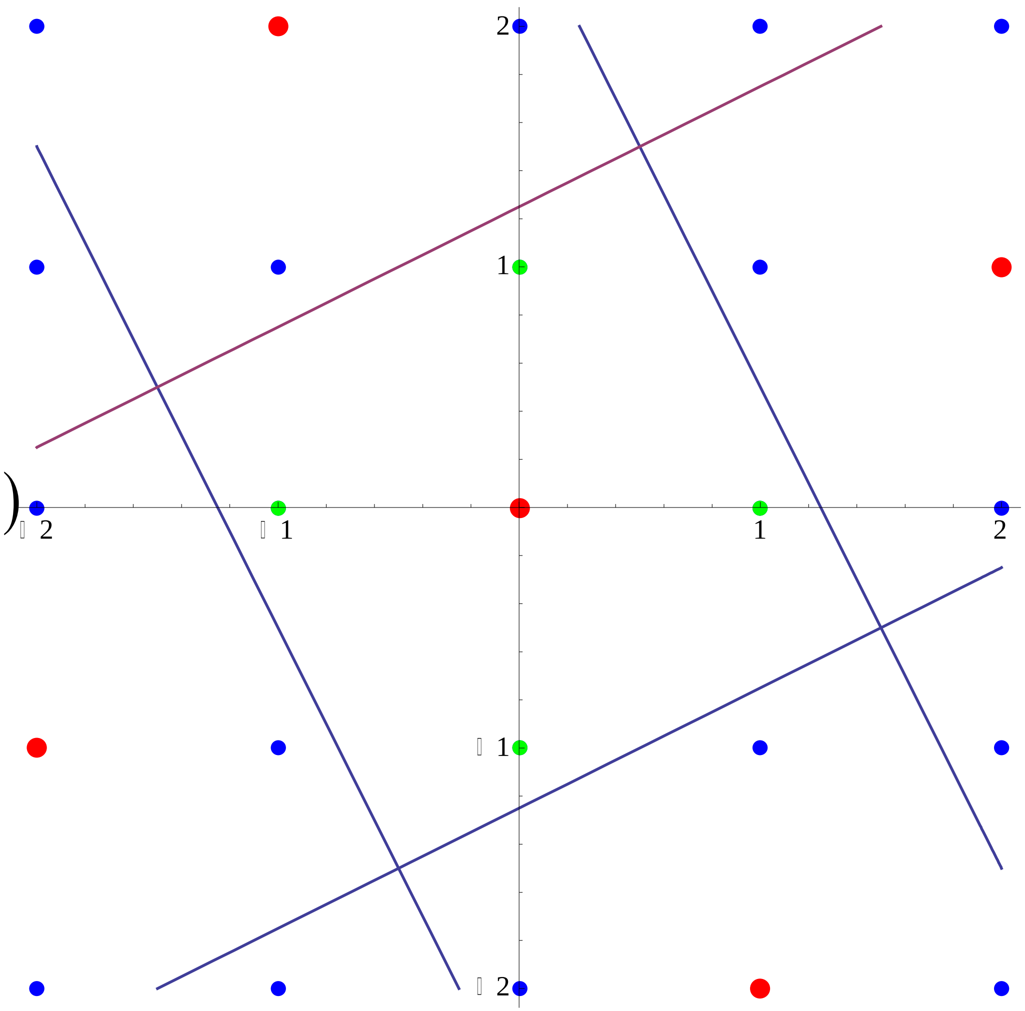
- Here we assume that each point in the coarse lattice is a point in the fine multiplied by some Gaussian integer q
  - i.e. the coarse is a scaled and rotated version of the fine
  - and the fine is just the Gaussian integers

$$\Lambda_c = q\mathrm{Z}\left[\mathrm{i}\right] \subset \Lambda = \mathrm{Z}\left[\mathrm{i}\right]$$

- We then define our signalling *constellation* as consisting of those Gaussian integers which fall in the Voronoi region of the coarse lattice

Example

- e.g. $q = 2 + \mathrm{i}$
- Blue points are fine lattice
- Red points are coarse lattice
- Fundamental region $V'(0)$ is region closer to origin than any other coarse lattice point
- Hence constellation is green points, plus origin
- $|q|^2 = 5$



Mapping

- This construction provides an isomorphic mapping between constellation points and a finite field or ring
  - a finite field if *q* is a Gaussian prime
  - a ring otherwise
  - in either case the size is $|q|^2$
- We can treat this as a quotient lattice:

$$\Lambda/\Lambda_c = \mathrm{Z}[i]/q\mathrm{Z}[i] \cong \begin{cases} \mathrm{F}_{|q|^2} & q \text{ prime} \\ \mathrm{R}\left(|q|^2\right) & \text{otherwise} \end{cases}$$

- If *q* is prime, can define a code over the field
- Again, minimum Euclidean distance limited by *q*

Practical issues

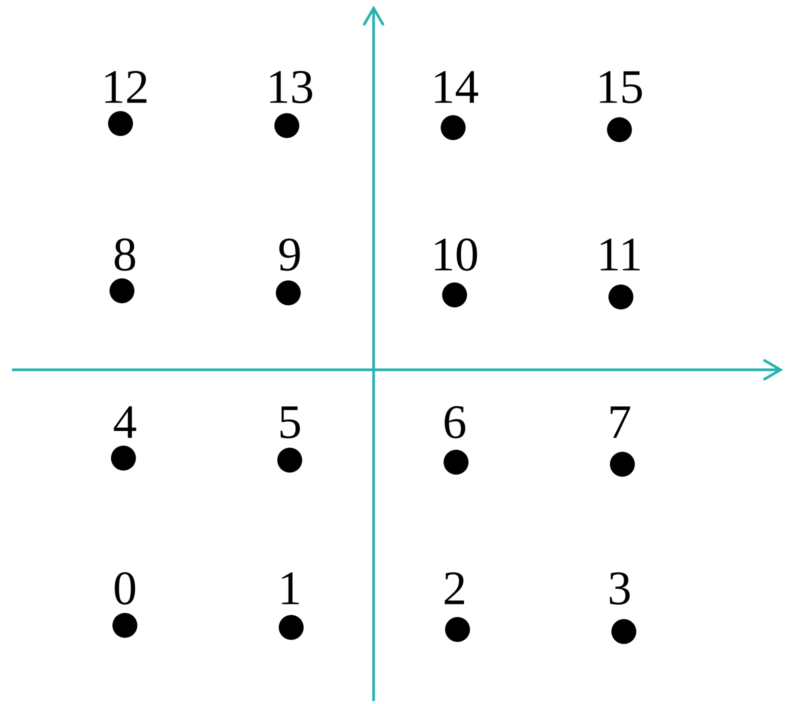
- We need relatively large q to construct useful lattice codes
  - then code radix is large
  - which typically makes decoding much more complex
- "Conventional" codes used in wireless communications are binary
  - often admit of simpler decoders
- Size of constellation given by $|q|^2$, either a prime or the square of a prime
  - "conventional" constellation size is a power of 2
  - difficult to map binary data to a prime constellation size
  - Only some constellation sizes are available

Outline

- Introduction: Lattices in wireless communications
- **Multilevel coded modulation**
- Multilevel lattices: the *elementary divisor construction*
- Multilevel lattice decoding
  - Layered Integer Forcing
  - Iterative decoding
- Conclusions

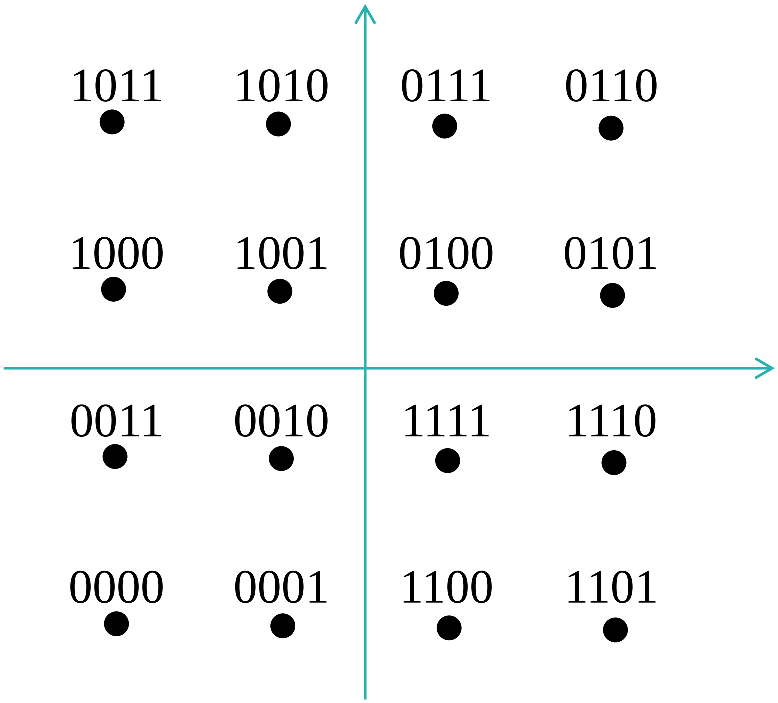
Encoding *M*-ary constellations

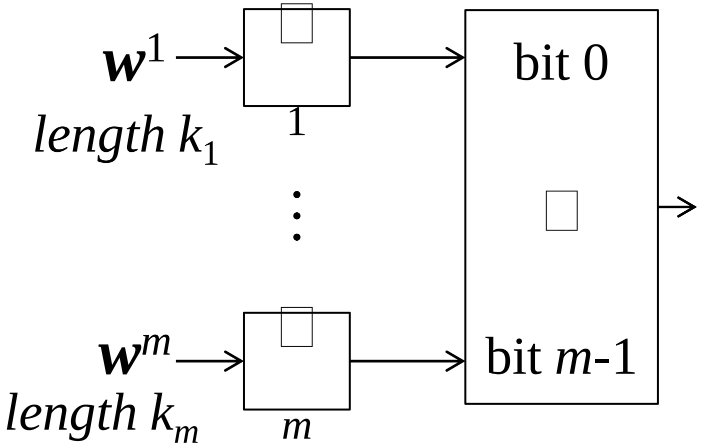
- More bandwidth-efficient wireless communications requires high order constellations – $M \gg 2$
- One approach would be to design an *M*-ary code to use with such constellations
  - however these tend to be either very complex
  - or to give poor performance
  - rarely used in practice
- Alternative is *multilevel coded modulation* (MLCM)



MLCM

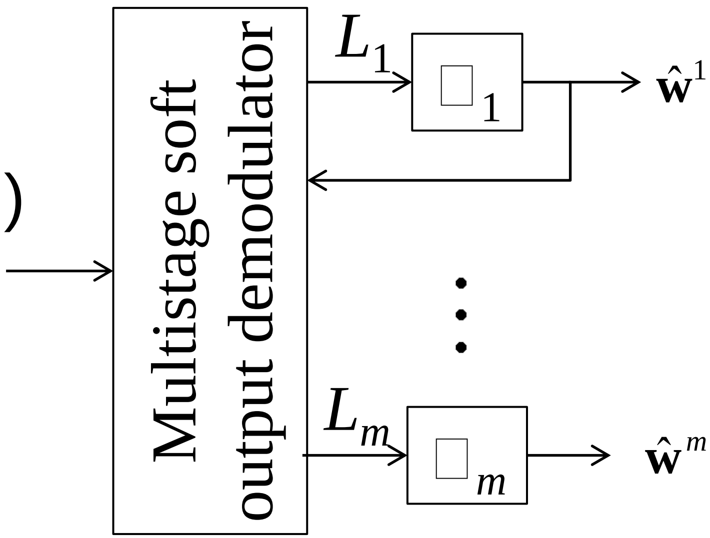
- In MLCM we devise a multi-symbol mapping scheme for the constellation
  - typically an M-point constellation with $M = 2^m$ is labelled with m-bit labels
  - we choose m length n binary codes, typically with different rates and minimum distance

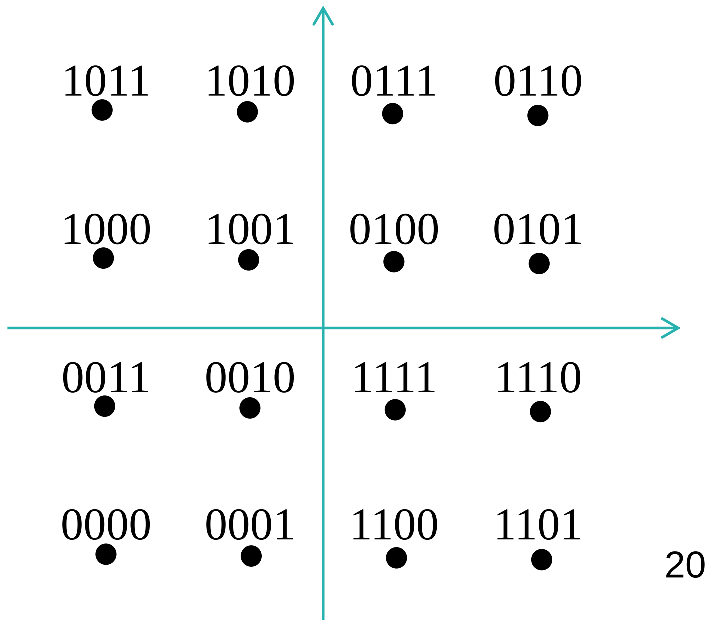




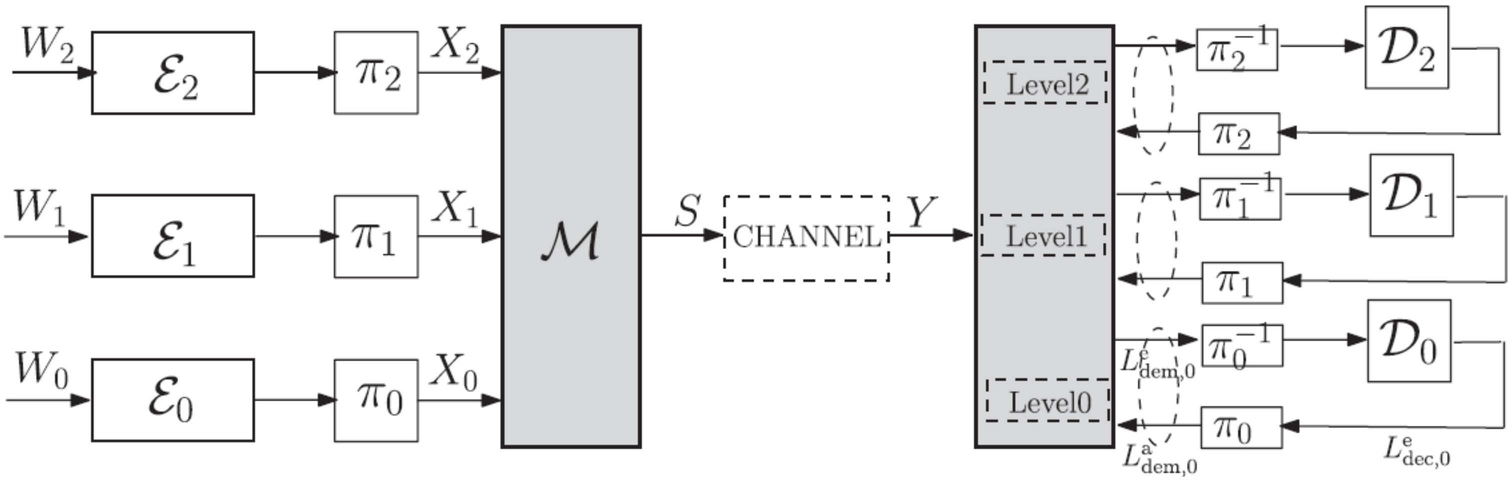
Multistage decoding

- This structure allows codes to be decoded in succession
- Soft output demodulator (SODem) generates likelihoods of code symbols
- Decoder $\square_1$ then attempts to decode level 1 code
  - feeds result back to SODem to help demodulate next level
  - and so on until level *m* is decoded
- Mapping may play important role





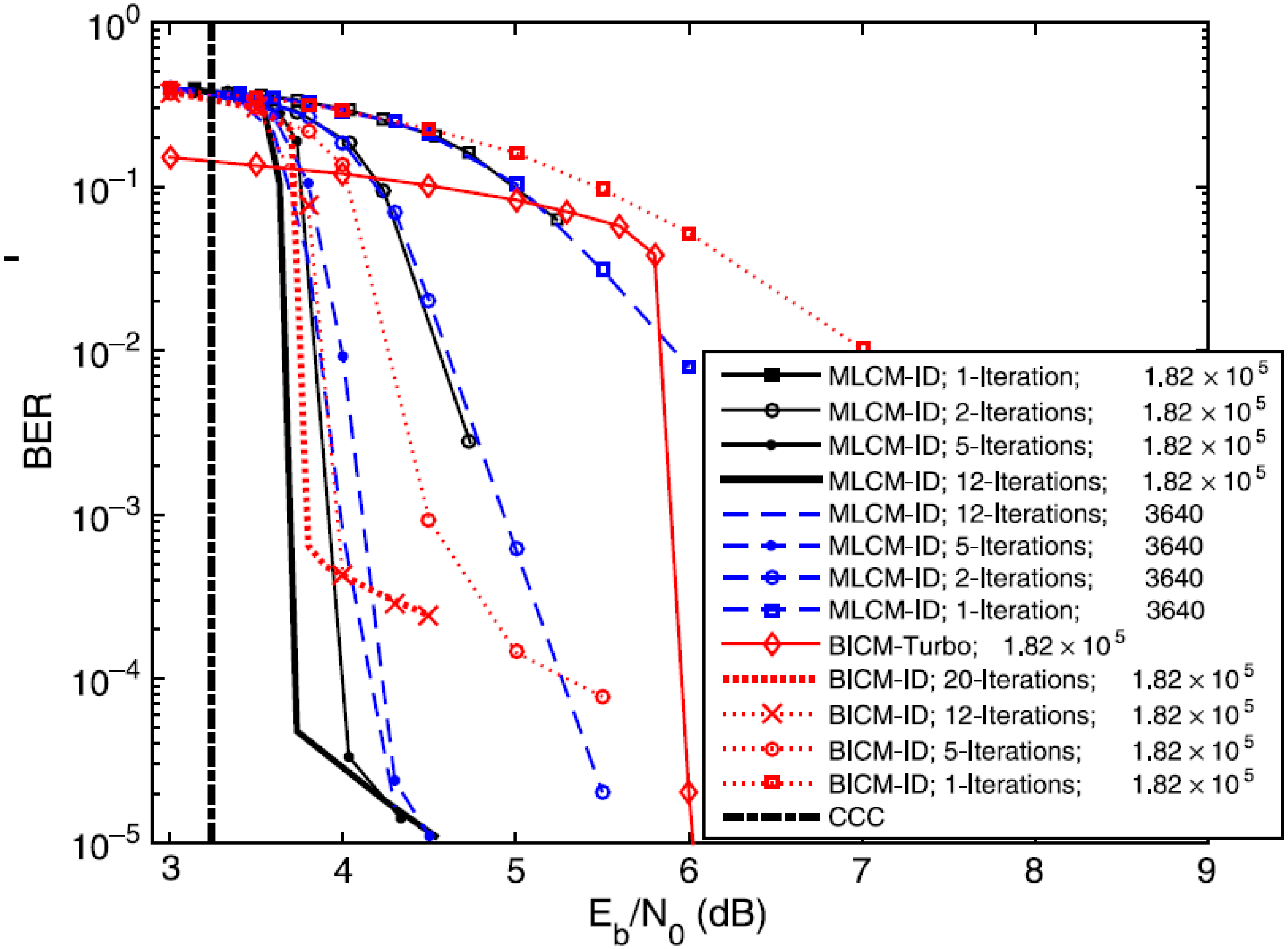
MLCM-ID



- Iterative Decoding further develops this by allowing several iterations of whole decoding process
  - similar to turbo decoding
  - gives performance close to Shannon bound, with appropriate choice of codes

Performance

- BER within 0.5 dB of Shannon (constellation-constrained) capacity
- with 12 iterations



Outline

- Introduction: Lattices in wireless communications
- Multilevel coded modulation
- **Multilevel lattices: the *elementary divisor construction***
- Multilevel lattice decoding
  - Layered Integer Forcing
  - Iterative decoding
- Conclusions

Multilevel Lattices

- We partition the quotient lattice into the direct sum of a series of ***primary sub-lattices***:
$$\Lambda/\Lambda' = \Lambda_{p_1}/\Lambda'_{p_1} \oplus \Lambda_{p_2}/\Lambda'_{p_2} \oplus \cdots \oplus \Lambda_{p_m}/\Lambda'_{p_m}$$
  - where $\Lambda_{p_i}/\Lambda'_{p_i} \triangleq \{\lambda \in \Lambda/\Lambda' : p_i^\gamma \lambda = 0\}$
  - and p_i is some prime in the PID on which the lattice is based (here we assume Gaussian or Eisenstein integers) and γ is some integer
- In each level of the partition we select elements of the quotient lattice which are *annihilated* by multiplication by some power of p_i
  - that is, they are reflected back onto the coarse lattice
- This operates in a similar way to mapping by set partitioning in MLCM

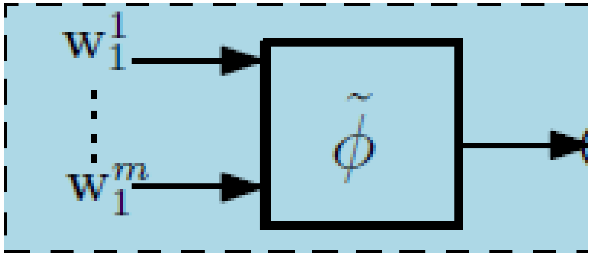
Mapping

- We can then define the isomorphism:

$$\Lambda_{p_i}/\Lambda'_{p_i} \cong S/\langle p_i^{\theta_1}\rangle \oplus S/\langle p_i^{\theta_2}\rangle \oplus \cdots \oplus S/\langle p_i^{\theta_t}\rangle$$

- (This is simplified in cases of practical interest to us in that only the first term is present)
- $S/\langle p_i^{\theta_1}\rangle$ is a quotient ring which is isomorphic either to a finite field (if θ =1) or a finite chain ring (otherwise)
- Thus the space of message symbols w^i at the i^{th} level is over this ring
- This provides a mapping ϕ_i between the quotient primary sub-lattice and a vector of data symbols:

$$\mathbf{w}^i = \bigoplus_j S/\langle p_i^{\theta_j}\rangle$$



Elementary Divisor Construction

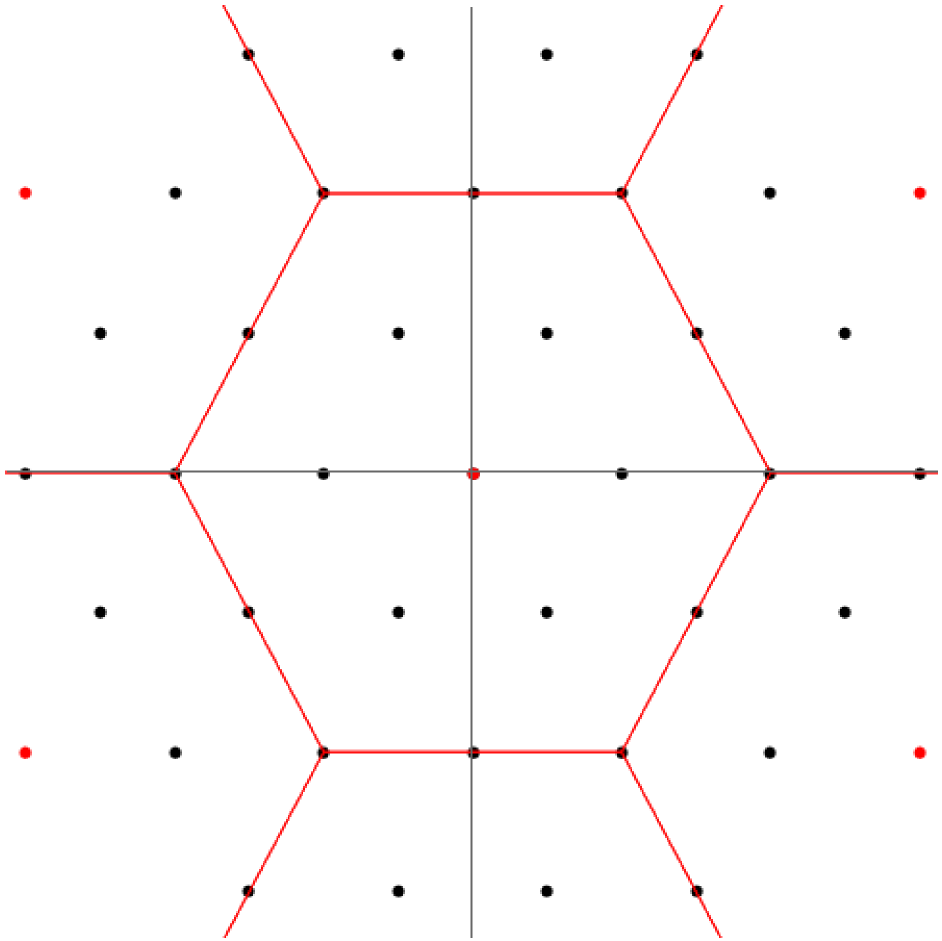
- So far this does not provide a practical means of constructing the lattices
- The *Elementary Divisor Construction* provides a means equivalent to Construction A/D to construct a lattice from a set of codes and a complex constellation
  - in fact it subsumes these constructions
- The fine lattice is defined as:

$$\Lambda \triangleq \{\lambda \in S^n : \tilde{\sigma}(\lambda) \in \mathcal{C}^1 \oplus \mathcal{C}^2 \oplus \cdots \oplus \mathcal{C}^m\}$$

  - where □^{1}, □^{2}…□^{m} denote the codes for each level, over corresponding ring/field
  - and $\sigma : S \longmapsto S/\langle p_1^{\gamma_1}\rangle \times S/\langle p_2^{\gamma_2}\rangle) \times \cdots \times S/\langle p_m^{\gamma_m}\rangle$ is a map (labelling scheme) defined by the partition of the PID by the primes $p_1, p_2 \ldots p_m$

Example

- Lattice based on Eisenstein integers □[ω], with $q = 2(1+2\omega)$, $p_1 = 2$, $p_2 = (1+2\omega)$
- Coarse lattice:
- Constellation cardinality $|q|^2 = 12$
- Because this is a ring rather than a field we cannot readily form a Construction A lattice
- Instead we partition into 2 quotient lattices based on p_1 and p_2

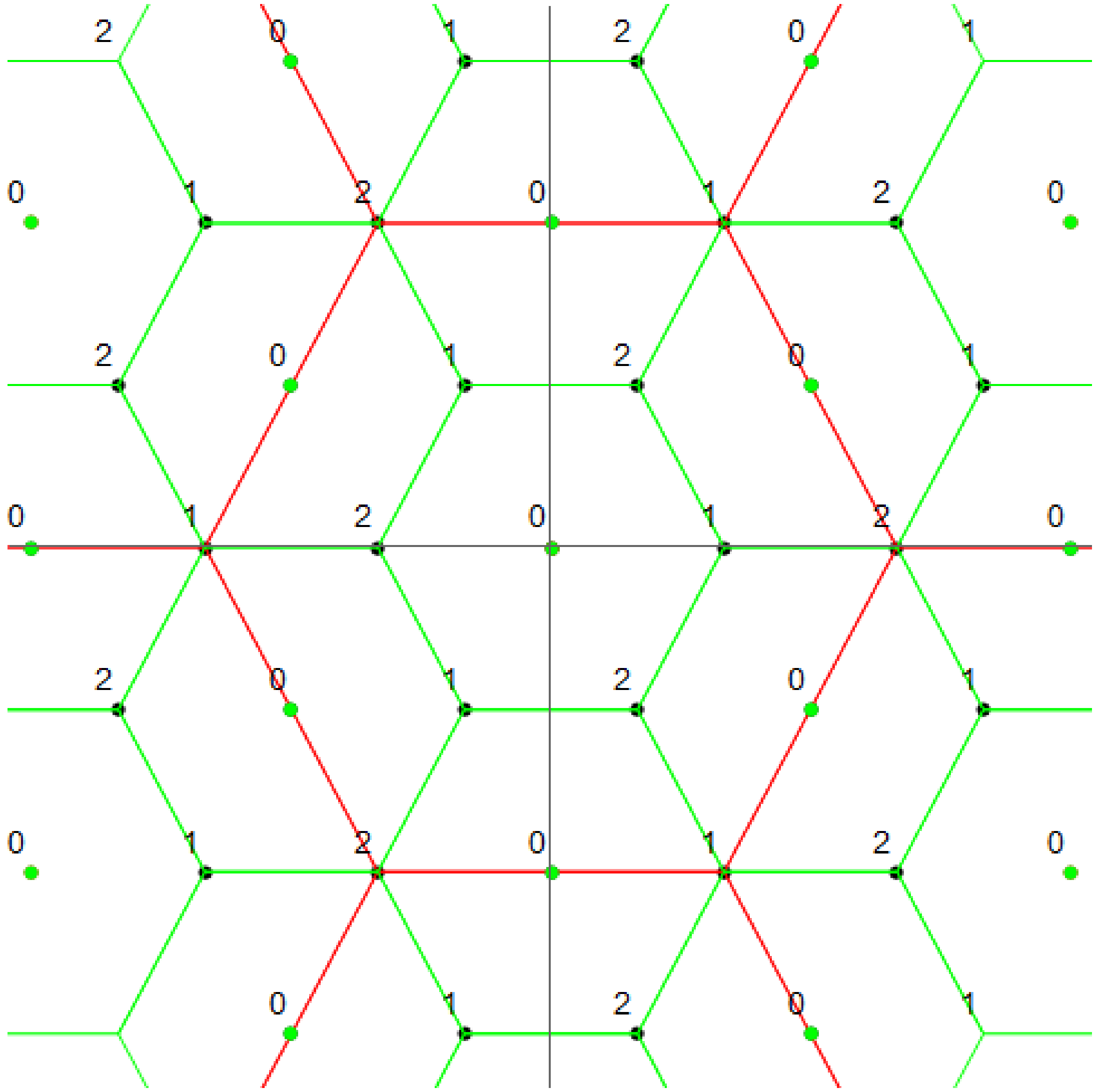


Level 1 lattice

- Cardinality of level 1 quotient lattice Λ_{p_1}/Λ' is

$$\frac{|q|^2}{|p_1|^2} = 3$$

- Provides first digit of constellation label

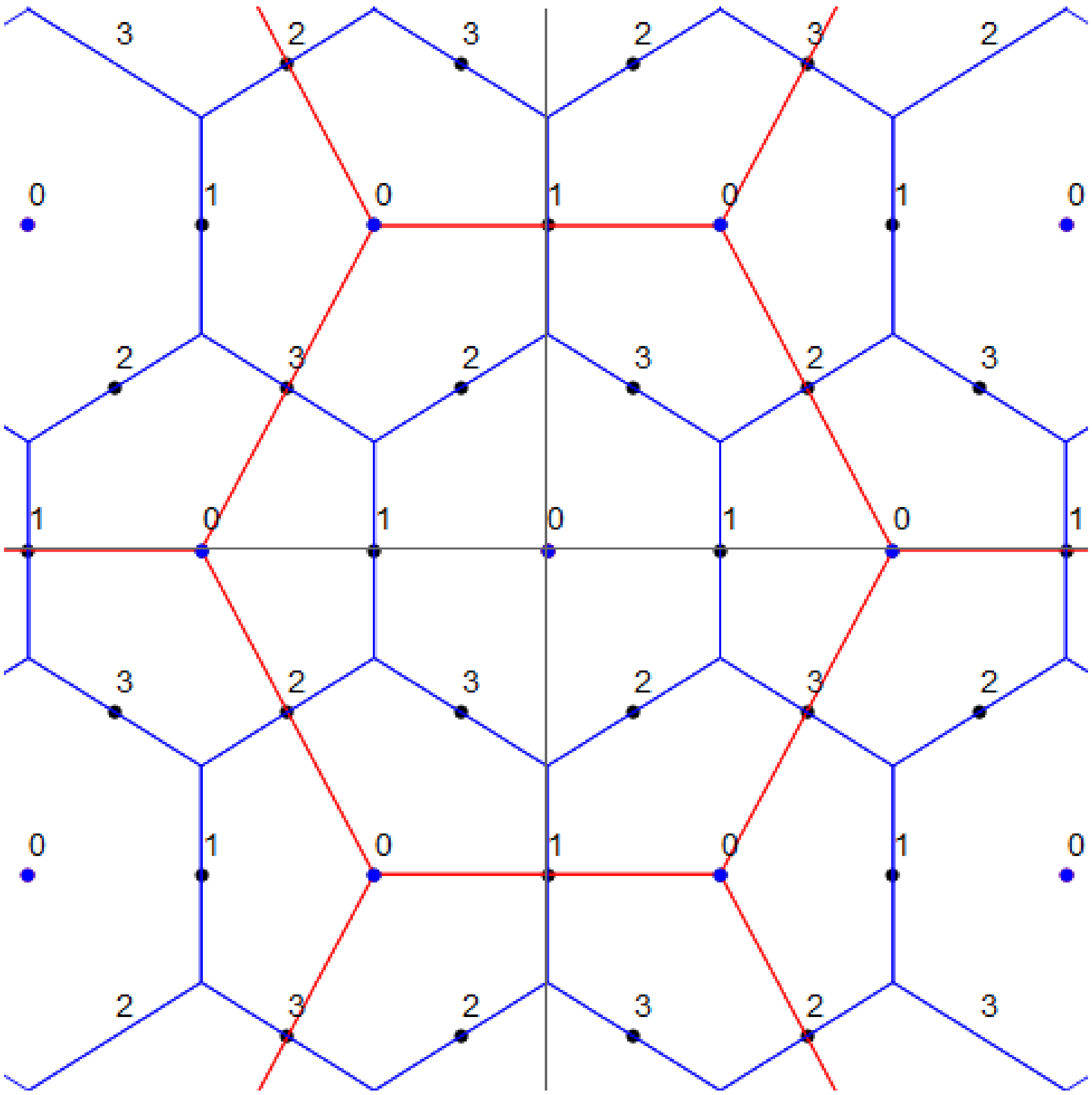


Level 2 lattice

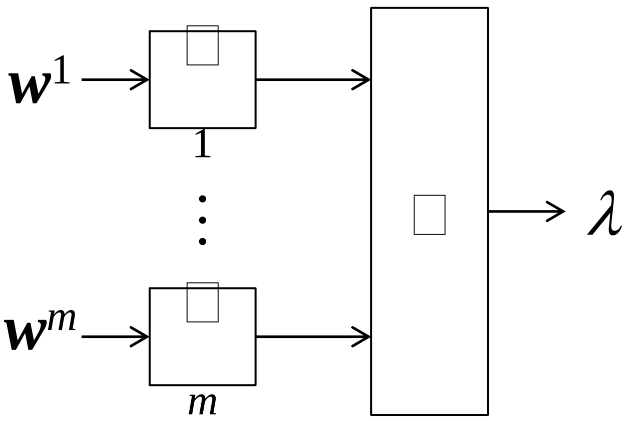
- Cardinality of level 2 quotient lattice Λ_{p2}/Λ' is

$$\frac{|q|^2}{|p_2|^2} = 4$$

- Provides second digit of constellation label



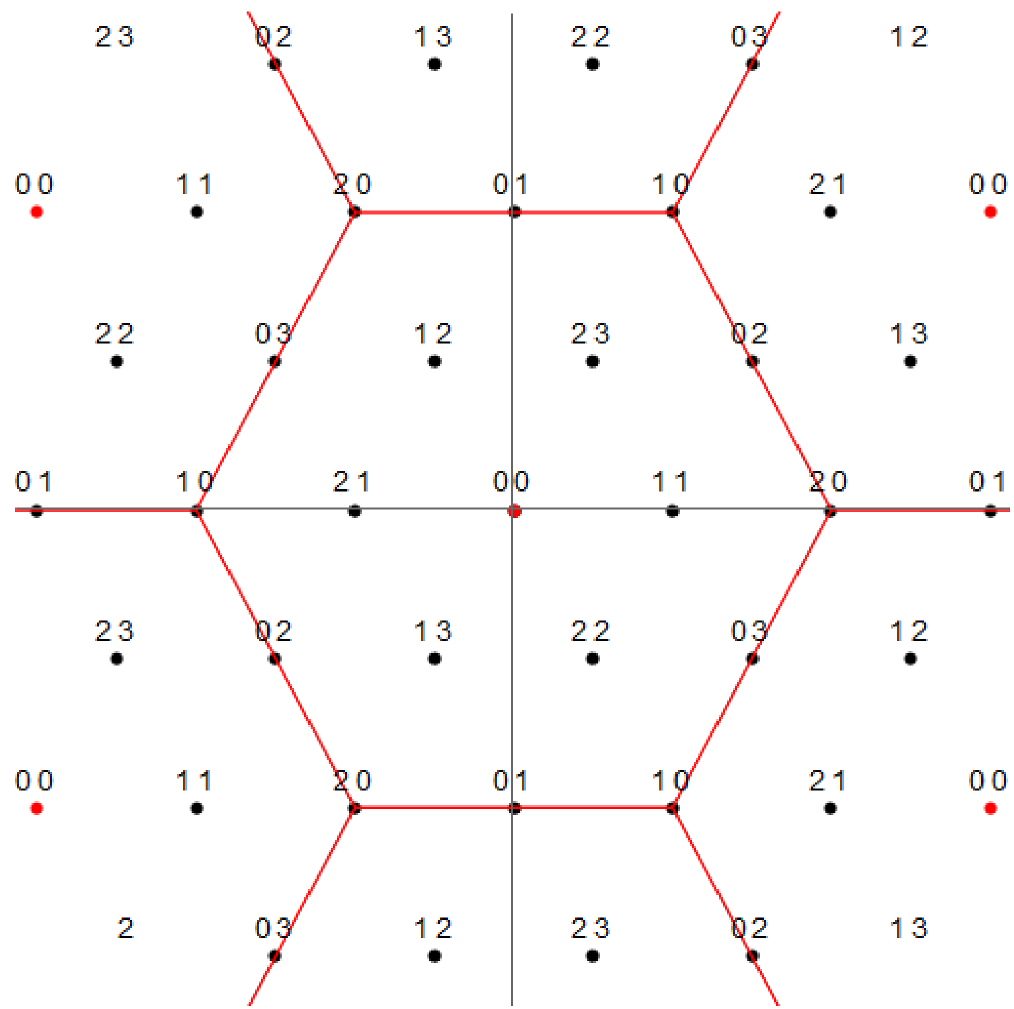
Encoding and Mapping



- Hence the partition provides a mapping scheme for the constellation
- In the example:

$$w^1 \in \square_3,\ w^2 \in \square_4$$

- Hence use two codes, on $\square_3$ and $\square_4$



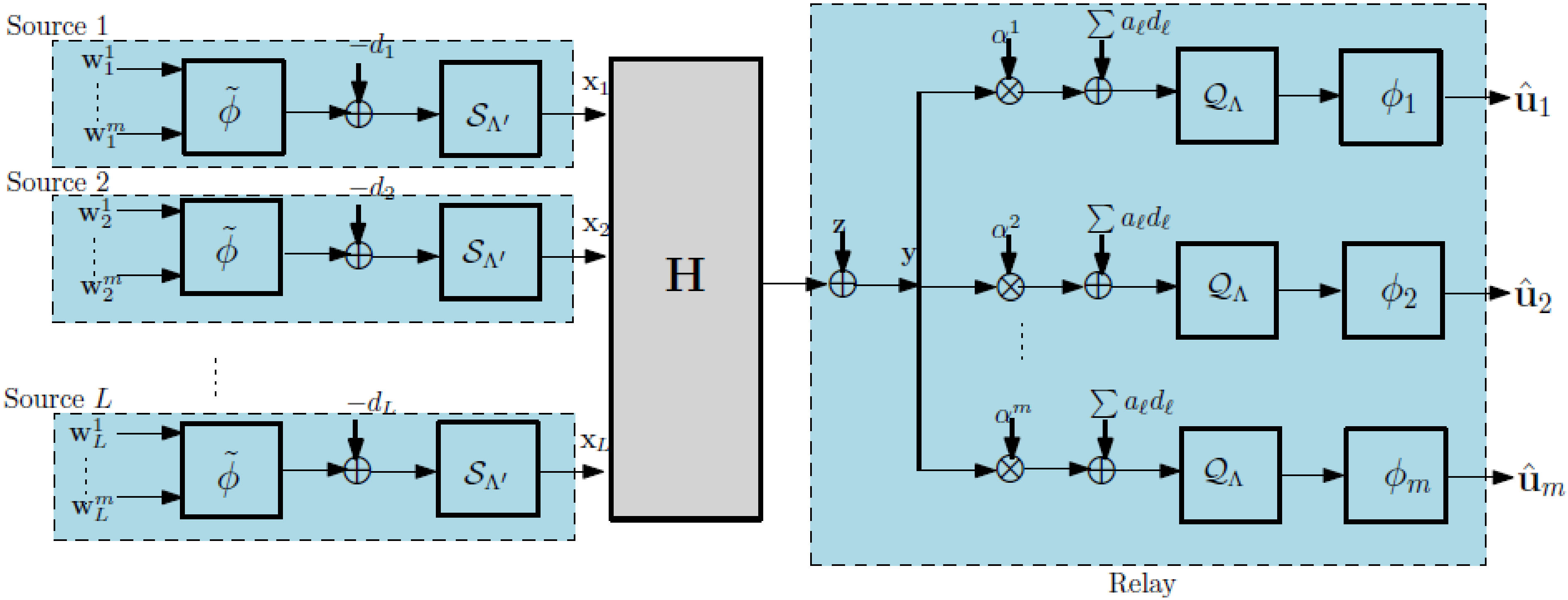
Outline

- Introduction: Lattices in wireless communications
- Multilevel coded modulation
- Multilevel lattices: the *elementary divisor construction*
- **Multilevel lattice decoding**
  - **Layered Integer Forcing**
  - **Iterative decoding**
- Conclusions

Multilevel lattice network code: decoding

- Multilevel structure also assists with decoding
  - allows each level to be decoded separately
  - with simpler decoder because of reduced cardinality
- Two approaches:
  - Layered Integer Forcing (LIF)
  - Multilevel decoding, one-shot or with iteration

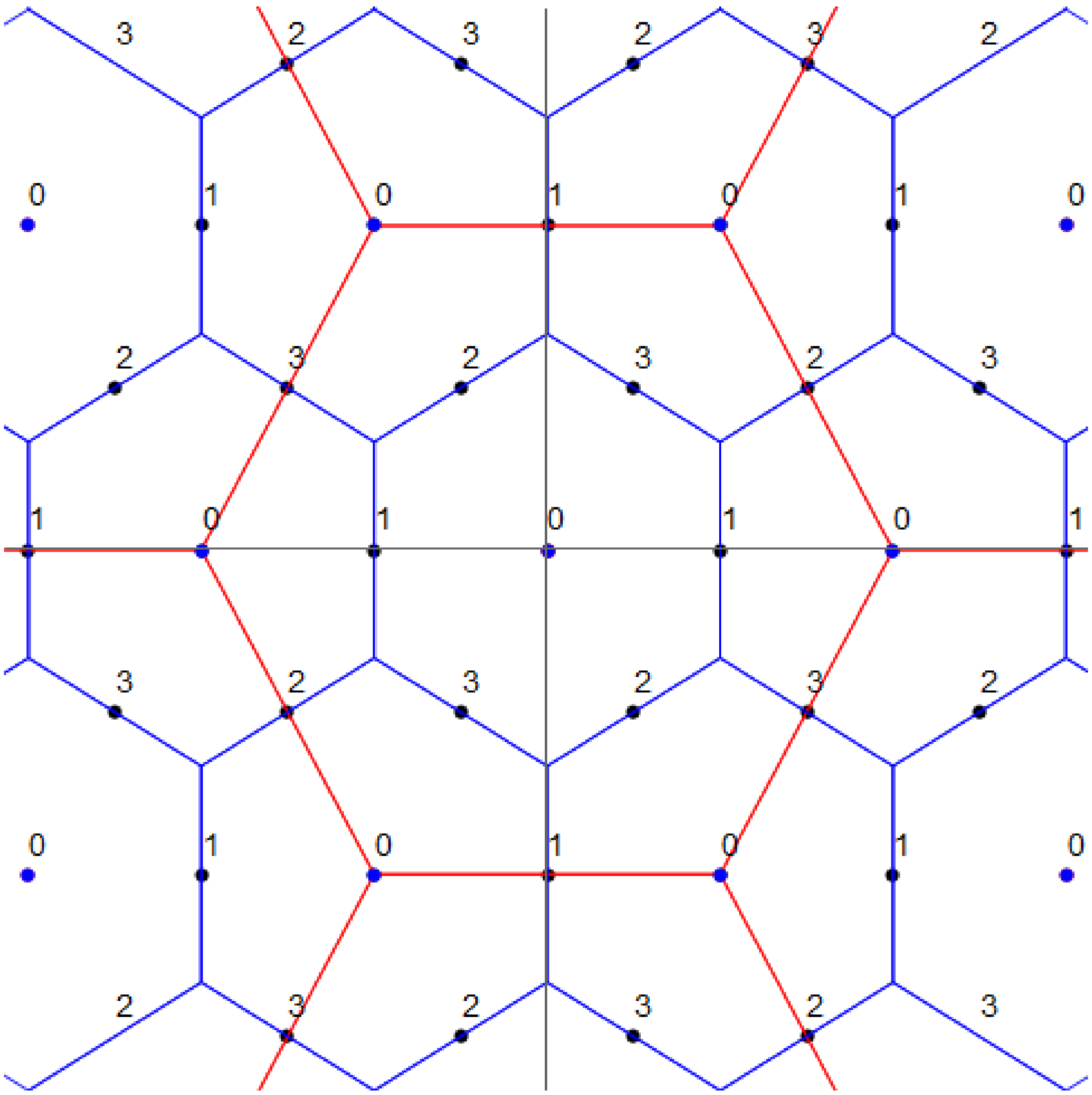
Layered Integer Forcing



- Transmitter: mapping, add dither, shaping
- Receiver: MMSE scaling (different for different levels), remove dither, quantise, demap
- On each level, can treat as a separate nested lattice code

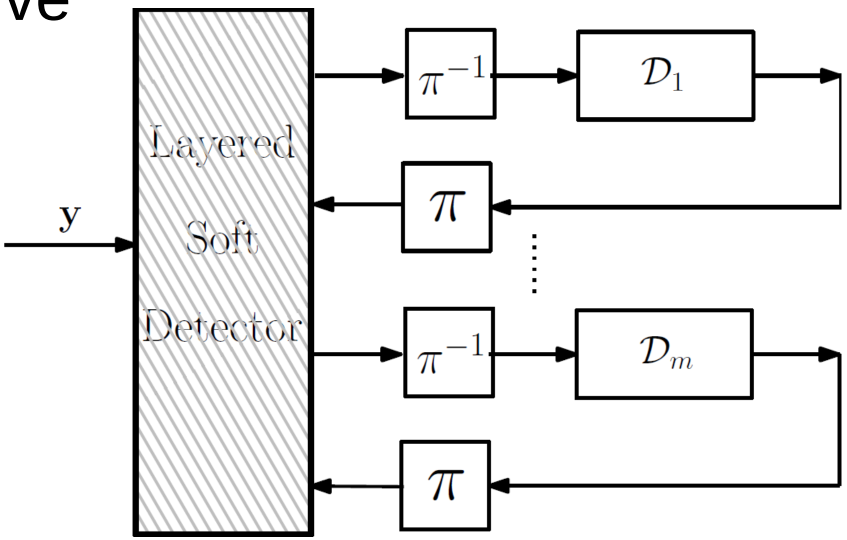
Level 2 decoding

- For example, we decode Level 2 independently of Level 1 by performing modulo-Λ_{p2} operation on received signal
  - rather than modulo- Λ'



Multilevel iterative decoding

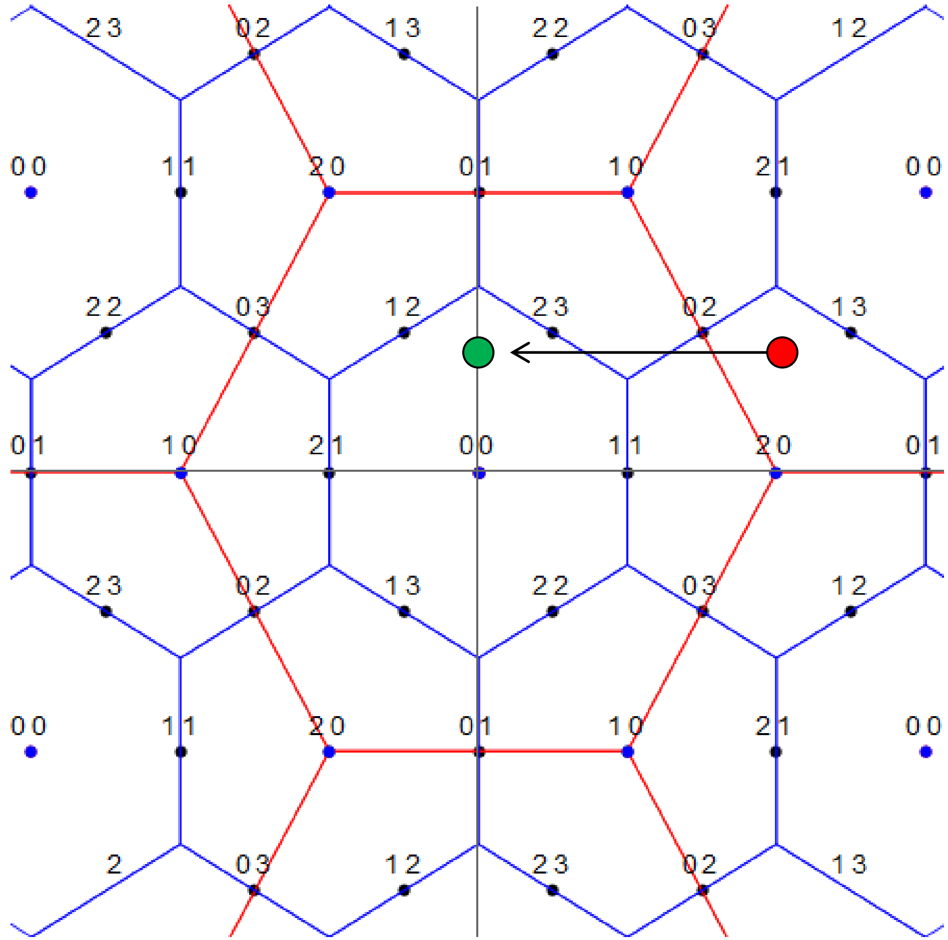
- We also introduce an alternative decoder based on soft output detection at each level
  - c.f. multistage decoding of MLCM
- Again we can use a one-shot multistage decoder
  - or apply multiple iterations of the decoding process



In the example – level 2

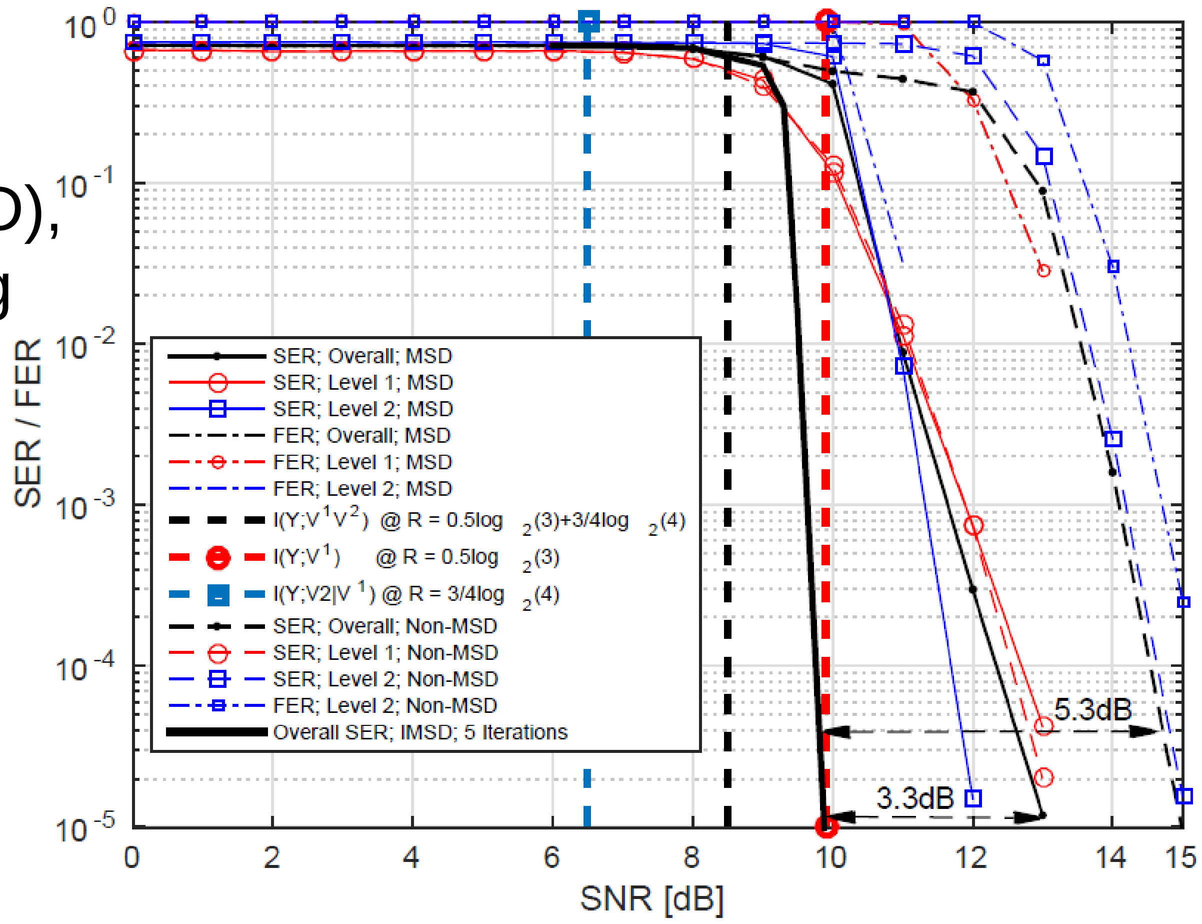
- *Received signal* (red dot)
- *After modulo-lattice* (green dot)

- Level 2 detector has information from level 1 decoder to assist
- e.g. if level 1 decoder indicates that ‘0’ more likely than ‘1’ at level 1, then level 2 detector will select ‘2’ rather than ‘3’



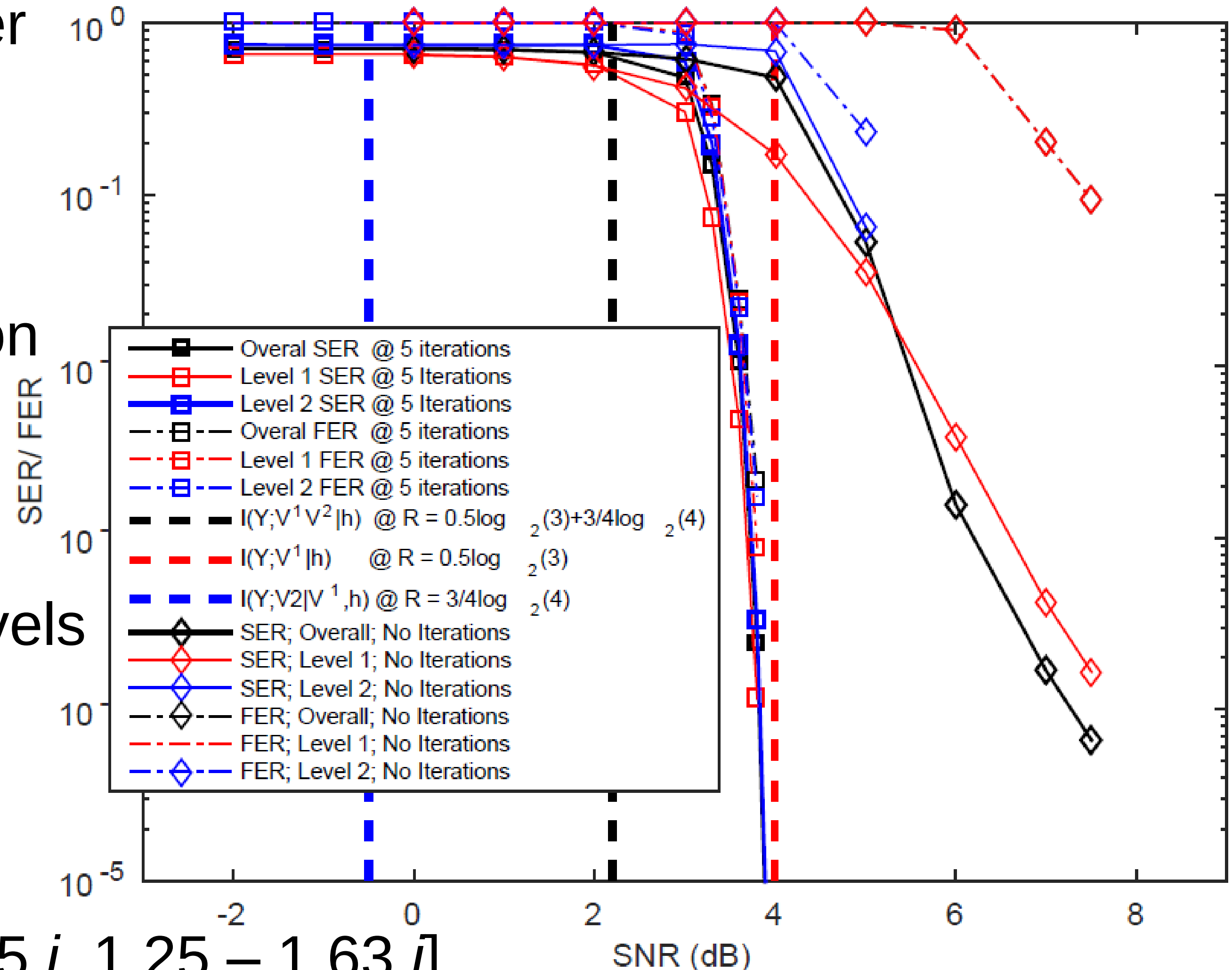
Performance

- Comparison of separate level decoding (Non-MSD), multistage decoding (MSD) and iterative decoding (IMSD)
- Shows how level 1 assists decoding of level 2
- Iteration results in “turbo-cliff” ~0.8 dB from capacity
- **h** = [1, 1]



Layered Integer Forcing

- Layered Integer Forcing with and without iterations
- Without iteration result a little worse than separate soft detection of levels
- With iteration, about 1.8 dB from capacity



- **h** = [1.17 + 2.15 *i*, 1.25 – 1.63 *i*]

Conclusions

- Multilevel lattice network coding has the potential to significantly reduce decoding complexity
  - compared to lattices based on Construction A
- Also provides much more flexibility in choice of constellation size
- We introduce *layered integer forcing* as a general approach for decoding general multilevel lattice codes
- Also the *elementary divisor construction* (EDC) for multilevel network codes based on codes
  - this subsumes Constructions A and D
  - also an iterative multistage decoding approach, which gives simulated performance close to capacity

Further work

- Note that we have presented here only one “flavour” of EDC
  - that in which each level is isomorphic to a finite field
- Other “flavours” have levels which are isomorphic to a finite chain ring
  - hybrid forms are also possible
- In these the level label is itself composite
- Note that in the ideal case the label would be binary, with constellation size a power of 2
  - allowing binary codes to be used
  - this may be possible for the finite chain ring form, with lattices based on Gaussian integers

References

- The presentation is based on two of our papers:
- Yi Wang and Alister Burr “Code Design for Iterative Decoding of Multilevel Codes” IEEE Trans. Communications, vol. 63, no. 7, July 2015, pp 2404-2419
- Yi Wang and Alister Burr “A Multilevel Framework for Lattice Network Codes” arxiv 1511.03297v1, 10 Nov 2015
  - also submitted to IEEE Trans. Information Theory
- The work was supported in part by EC FP7 contract no. 31877 “DIWINE”