Aalto University
School of Science
and Technology

Coding Theory on Non-Standard Alphabets

Group testing with error correction

Marcus Greferath

Department of Mathematics and Systems Analysis
Aalto University School of Sciences
marcus.greferath@aalto.fi

June 2023

Partially Ordered Sets (Posets)

Definition

A binary relation $\leq$ on a non-empty set P is called a partial order if it satisfies:

R: $x \leq x$ for all $x \in P$.

A: $x \leq y$ and $y \leq x$ implies $x = y$ for all $x, y \in P$.

T: $x \leq y$ and $y \leq z$ implies $x \leq z$ for all $x, y, z \in P$.

The pair $(P, \leq)$ is then called a partially ordered set.

From a variety of examples we mention a few:

- the subset relation $\subseteq$ on a power set 2^X,
- the natural orders $\leq$ on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$,
- the divisibility relation $|$ on $\mathbb{N}$.

Residuated Mappings on Posets

Definition

Let $(A, \leq)$ and $(B, \preceq)$ be partially ordered sets. For mappings $f : A \longrightarrow B$ and $g : B \longrightarrow A$, the pair (f, g) is called a residuated pair, if there holds

$$(\star) \quad f(a) \preceq b \iff a \leq g(b) \ \text{ for all } a \in A \text{ and } b \in B.$$

Here, f is said to be residuated, while g is called residual.

Residuation Theory may be considered as an abstraction of the concept of Galois correspondence.

It is nicely developed in T. S. Blyth' and M. F. Janowitz' book on Residation Theory.

Residuated Mappings on Posets (cont'd)

In the mentioned book by Blyth and Janowitz, residuated mappings are defined in a different way. The following will clarify the connection.

Definition

Let $(A, \leq)$ and $(B, \preceq)$ be partially ordered sets. A mapping $f : A \longrightarrow B$ is called isotone, if

$$x \leq y \quad \text{implies} \quad f(x) \preceq f(y) \quad \text{for all } x, y \in A.$$

Theorem

Let $(A, \leq)$ and $(B, \preceq)$ be partially ordered sets. For mappings $f : A \longrightarrow B$ and $g : B \longrightarrow A$ the following are equivalent:

- *(f, g) is a residuated pair.*
- *f and g are isotone, and $g(f(a)) \geq a$ and $f(g(b)) \preceq b$ for all $a \in A$ and $b \in B$.*

Proof of the Theorem

Part A: Assume first that (f, g) forms a residuated pair.

1: For $a \in A$ we have $f(a) \preceq f(a)$ which leads to $a \leq g(f(a))$ by a single use of $(\star)$.

2: For $b \in B$ we have $g(b) \leq g(b)$ which leads to $f(g(b)) \preceq b$, again using $(\star)$.

3: Now let $s, a \in A$ with $s \leq a$. From $a \leq g(f(a))$ we obtain $s \leq g(f(a))$, which by $(\star)$ leads to $f(s) \preceq f(a)$.

4: Similarly, let $t, b \in B$ with $t \preceq b$. From $f(g(t)) \preceq t$ we obtain $f(g(t)) \preceq b$, which by $(\star)$ leads to $g(t) \leq g(b)$.

Proof of the Theorem (cont'd)

Part B: Assume now that f and g are isotone with $g(f(a)) \geq a$ and $f(g(b)) \preceq b$ for all $a \in A$ and $b \in B$.

1: Let $a \in A$ and $b \in B$ be given with $f(a) \preceq b$. By g being isotone, we find $g(f(a)) \leq g(b)$. Together with $a \leq g(f(a))$ this shows $a \leq g(b)$, as desired.

2: Let now $a \in A$ and $b \in B$ be given with $a \leq g(b)$. By f being isotone, we find $f(a) \preceq f(g(b))$. Combining this with $f(g(b)) \preceq b$, we find $f(a) \preceq b$, again as desired.

3: Combining 1: and 2: we obtain condition $(\star)$, which finishes the proof. □

Agreement: Relying on mathematical maturity and the fact that confusion will be impossible, we will use the generic simple symbol $\leq$ for all further occurring partial order relations.

Further Properties of Residuated Mappings

Let $f : A \longrightarrow B$ be a residuated mapping.

1: The residual mapping $g : B \longrightarrow A$ is uniquely determined by f. Dually, f is uniquely determined by its residual g.

2: $f \circ g \circ f = f$ and $g \circ f \circ g = g$. Therefore $g \circ f(a) = a$ for all $a \in \mathrm{im}(g)$ and $f \circ g(b) = b$ for all $b \in \mathrm{im}(f)$.

3: Call the elements of $H := \mathrm{im}(g)$ closed elements in A and dually the elements of $K := \mathrm{im}(f)$ kernel elements in B. Then 2: says, that $f_{|H}$ and $g_{|K}$ are mutually inverse.

Definition

A poset $(L, \leq)$ is called a complete lattice if for every subset $X \subseteq L$ there exists a smallest upper bound denoted by $\sum X$ and a greatest lower bound denoted by $\prod X$ in L.

Further Properties (cont'd)

Let $f : A \longrightarrow B$ be a residuated mapping.

4: If A and B are complete lattices, then f is residuated if and only if $f(\sum X) = \sum f(X)$ for all $X \subseteq A$. Accordingly g is a residual mapping iff $g(\prod Y) = \prod g(Y)$ for all $Y \subseteq B$.

5: In this case, we can directly write down a closed form of g, namely

$$g(b) \ = \ \sum \{a \in A \mid f(a) \leq b\}.$$

Consider the (complete) lattice $\mathbb{B}_2 := \{0, 1\}$ with order $0 \leq 1$. Its $\sum$ and $\prod$ operations are represented by $+$ and $\cdot$ in the tables:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Figure: Operation tables of the binary semifield $\mathbb{B}_2$

Further Properties (cont'd)

As a matter of fact, $\mathbb{B}_2$ is also referred to as the binary semifield. Consequently, we may talk of a vectorspace when referring to $\mathbb{B}_2^n$.

6: Any residuated mapping $f : \mathbb{B}_2^n \longrightarrow \mathbb{B}_2^k$ can be represented by a $n \times k$ matrix M with entries in $\mathbb{B}_2$, such that

$$f([x_1, \ldots, x_n]) = [x_1, \ldots, x_n] \cdot M$$

for all $[x_1, \ldots, x_n] \in \mathbb{B}_2^n$.

Recall that $\mathbb{B}_2$ comes with a negation $N : \mathbb{B}_2 \longrightarrow \mathbb{B}_2,\ x \mapsto \overline{x}$, where $\overline{0} = 1$ and $\overline{1} = 0$.

We will extend this negation to $\mathbb{B}_2^n$ componentwise, and refrain from using new notation: Hence, we have

$$\overline{[x_1, \ldots, x_n]} \;=\; [\overline{x_1}, \ldots, \overline{x_n}]\,.$$

Further Properties (cont'd)

We will now be show how to describe the residual mapping g for a given residuated mapping $f : \mathbb{B}_2^n \longrightarrow \mathbb{B}_2^k$.

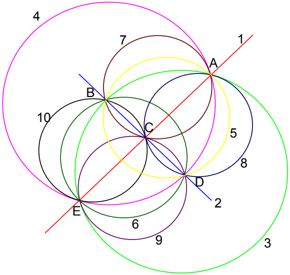
7: Let M be a $n \times k$-matrix representing a residuated mapping $f : \mathbb{B}_2^n \longrightarrow \mathbb{B}_2^k$. Then the residual mapping is given by $g : \mathbb{B}_2^k \longrightarrow \mathbb{B}_2^n,\ y \mapsto \overline{\overline{y} \cdot M^T}$.

Proof: (Sketch only) The negation operator N reverts the order $\leq$ on all vectorspaces involved. Due to this, residuated mappings become residual, while residual mapping become residuated. g as a now residuated mapping will then enjoy a matrix representation by a $k \times n$-matrix derived from M. To see that M^T is the right candidate is a bit tedious and exceeds our time frame. □

What is Group Testing?

- Group testing is a method to exploit testing resources efficiently, when they are complicated or costly.
- Around 1943 it was developed by R. Dorfman and enjoyed a matrix-based formalization by Katona in 1973.
- The underlying idea is that each test is used for a pool of fractions from different samples, while the individual samples are spread over different pools.
- We assume that we have only one round of testing, an approach known as non-adaptive group testing.

A small example



	1	2	3	4	5	6	7	8	9	10
A	1	0	1	1	1	0	1	1	0	0
B	0	1	1	0	1	1	1	0	0	1
C	1	1	0	0	0	0	1	1	1	1
D	0	1	0	1	1	1	0	1	1	0
E	1	0	1	1	0	1	0	0	1	1

- To organize group tests it is useful to have a table (a binary matrix) for tests and samples showing which sample is participating in which pool.
- The scheme at hand allows to identify a single infected sample out of 10, using 5 tests.
- For more than one infected sample, the scheme may fail.

Group Testing

- For example, assuming that exactly sample 3 is infected, we find that:

$$\begin{bmatrix} 0\,0\,1\,0\,0\,0\,0\,0\,0\,0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,0\,1 \end{bmatrix}.$$

- This means, that test A, B, and E will be positive, while the remaining tests will show a negative result.

- Will the resulting vector $\begin{bmatrix} 1\,1\,0\,0\,1 \end{bmatrix}$ uniquely identify sample 3 as infected?

Group Testing (cont'd)

- Well, this could be checked here by hand. However, applying what we have just learnt we compute:

$$\overline{\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \end{bmatrix}} \cdot \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

- Negation of the result yields the vector $\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$, which was expected, or at least desired.

- This went well, because vectors of Hamming weight 1 in $\mathbb{B}_2^{10}$ are closed elements regarding the residuated mapping that is represented by the above test matrix.

- What might happen, if we have two infected samples?

An Illustration

- **Example:** Show that vectors of Hamming weight 2 in $\mathbb{B}_2^{10}$ are not generally closed regarding the above mapping.

- Look for example at the infection pattern $\begin{bmatrix}1&0&1&0&0&0&0&0&0&0\end{bmatrix}$ saying that sample 1 and 3 are infected.

- Here all tests will be positive, except test D, so that we have $\begin{bmatrix}1&1&1&0&1\end{bmatrix}$ as group testing result.

- Like before, we compute

$$\overline{\begin{bmatrix}1&1&1&0&1\end{bmatrix}} \cdot \begin{bmatrix}1&0&1&1&1&0&1&1&0&0\\0&1&1&0&1&1&1&0&0&1\\1&1&0&0&0&0&1&1&1&1\\0&1&0&1&1&1&0&1&1&0\\1&0&1&1&0&1&0&0&1&1\end{bmatrix} = \begin{bmatrix}0&1&0&1&1&1&0&1&1&0\end{bmatrix}.$$

and obtain the vector $\begin{bmatrix}1&0&1&0&0&0&1&0&0&1\end{bmatrix}$ after negation.

An Illustration (cont'd)

- This vector $\begin{bmatrix}1&0&1&0&0&0&1&0&0&1\end{bmatrix}$ and a quick look at the test matrix indicate, that any (infected) subset of size at least 2 of the set $\{1, 3, 7, 10\}$ could have caused the result given.
- This might be considered sub-optimal, but it shows that we are fighting false positives, and never false negatives.
- **Conclusion:** The main goal of group testing is the con- struction of residuated mappings on $f : \mathbb{B}_2^n \longrightarrow \mathbb{B}_2^k$, such that k is as small as possible, and that any vector of Hamming weight $\leq d$ is closed, where d is as large as possible.
- These mappings might be referred to as (n, k, d)-group testing schemes.

d-separability and d-disjunctness

For what follows, let $B_n(x, d)$ denote the Hamming disk of radius d centered in $x \in \mathbb{B}_2^n$. Moreover $B := \{e_1, \ldots, e_n\}$ shall denote the standard basis of $\mathbb{B}_2^n$, i.e. the non-zero elements of $B_n(0, 1)$.

Definition

Let f be an (n, k) group testing scheme. For a natural number d consider the following properties:

- **d**-sep: The restriction of f to $B_n(0, d)$ is injective.
- **d**-dis: For any t-element subset T of B and any $y \notin T$ there holds $f(y) \not\leq \sum f(T)$, as long as $t \leq d$.
- **d**-rev: If $x \in B_n(0, d)$ and $y \in \mathbb{B}_2^n$, then $f(x) = f(y)$ will imply $x = y$.

Remark: From the literature we obtain the well-known facts:

(i) **d**-dis implies **d**-sep, and

(ii) $\mathbf{d+1}$-sep implies **d**-dis.

d-separability and d-disjunctness (cont'd)

Theorem

Let f be an (n,k) group testing scheme, and let g denote the residual mapping of f. Then the following are equivalent:

- **(a)** *f satisfies* **d**-*rev.*
- **(b)** *f satisfies* **d**-*dis.*
- **(c)** $B(0,d) \subseteq \mathrm{im}(g)$.
- **(d)** $g \circ f(x) = x$ *for all* $x \in B_n(0,d)$.

Theorem

Let H be the $n \times k$ matrix representing an (n,k) group testing scheme f. Then the following are equivalent:

- **(a)** *f satisfies* **d**-*rev.*
- **(b)** $B(1,d) \subseteq \mathrm{colspace}(H)$.

Incidence Structures and Incidence Matrices

For most of what follows, let (P, B) be an incidence structure on the v-element set P of points, and let $b = |B|$ denote the number of blocks of B.

Definition

A binary matrix $M \in \mathbb{B}_2^{b\times v}$ is called an incidence matrix for (P, B), if its rows are labelled by the blocks, while its columns are labelled by the points of (P, B), such that

$$M_{c,p} = \begin{cases} 1 & : \quad p \in c, \\ 0 & : \quad \text{otherwise.} \end{cases}$$

Incidence matrices may thus be considered as indicator functions of their underlying incidence relation.

Partial Linear Spaces

Definition

For natural number s and t, a finite incidence structure (P, L) consisting of points and lines is called a partial linear space of order (s, t) if the following axioms hold:

- Two different points are connected by at most one line.
- Every line is incident with $s + 1$ points, and every point is incident with $t + 1$ lines.

Note: Interchanging the terms “line” and “point” will transform a partial linear space of order (s, t) into a partial linear space of order (t, s).

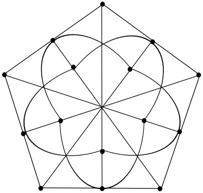
This comes from the fact, that any two lines in a partial linear space may intersect in at most one point.

Generalized Quadrangles

A well-understood class of partial linear spaces is that of the generalized quadrangles, first introduced by J. Tits.

Definition

A partial linear space (P, L) of order (s, t) is called a generalized quadrangle, denoted by $GQ(s, t)$, if for any non-incident point-line pair (p, ℓ), there exists a unique point q on ℓ that is connected with p by a line.



Remark: A generalized quadrangle of order (s, t) has $(s + 1)(st + 1)$ points and $(t + 1)(st + 1)$ lines.

Figure: GQ(2,2) aka W(2)

Group Testing Schemes from Partial Linear Spaces

The proof of the following result is rather simple, so we leave it to the interested audience.

Theorem

Let (P, L) be a partial linear space of order (s, t), and let $\ell_1, \dots \ell_m$ denote a collection of m distinct lines in L. If $\ell \in L$ is a line with $\ell \subseteq \ell_1 \cup \cdots \cup \ell_m$ then $\ell = \ell_j$ for some $1 \leq j \leq m$ provided $m \leq s$.

For the incidence matrix of a partial linear space (P, L) we may derive the following immediate conclusion.

Corollary

The group testing scheme resulting from the incidence matrix of a partial linear space of order (s, t) satisfies condition $\mathbf{t}$-rev.