Prolific IPP Codes

Simon R. Blackburn
Joint work with Tuvi Etzion and Siaw-Lynn Ng

Royal Holloway, University of London

11th December 2007

Overview

Some definitions

Notation: F is a finite set of size q, and ℓ is a positive integer.

Definition

Let $x, y \in F^\ell$. The set of descendants of $\{x, y\}$ is the set:

$$\mathrm{Desc}(\{x, y\}) = \{d \in F^n \mid \forall i \in \{1, 2, \ldots, \ell\},\ d_i \in \{x_i, y_i\}\}.$$

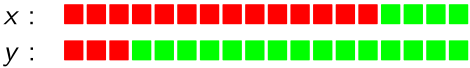
Some definitions

Notation: F is a finite set of size q, and ℓ is a positive integer.

Definition

Let $x, y \in F^\ell$. The set of descendants of $\{x, y\}$ is the set:

$$\mathrm{Desc}(\{x, y\}) = \{d \in F^n \mid \forall i \in \{1, 2, \ldots, \ell\},\ d_i \in \{x_i, y_i\}\}.$$



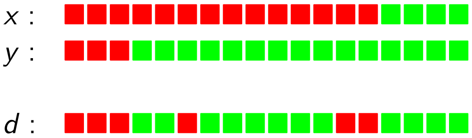
Some definitions

Notation: F is a finite set of size q, and ℓ is a positive integer.

Definition

Let $x, y \in F^\ell$. The set of descendants of $\{x, y\}$ is the set:

$$\mathrm{Desc}(\{x,y\}) = \{d \in F^n \mid \forall i \in \{1,2,\ldots,\ell\},\ d_i \in \{x_i, y_i\}\}.$$



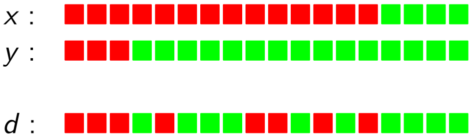
Some definitions

Notation: F is a finite set of size q, and ℓ is a positive integer.

Definition

Let $x, y \in F^\ell$. The set of descendants of $\{x, y\}$ is the set:

$$\mathrm{Desc}(\{x, y\}) = \{d \in F^n \mid \forall i \in \{1, 2, \ldots, \ell\}, \ d_i \in \{x_i, y_i\}\}.$$



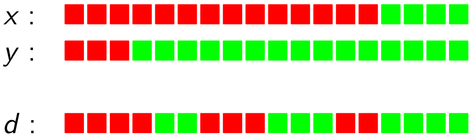
Some definitions

Notation: F is a finite set of size q, and ℓ is a positive integer.

Definition

Let $x, y \in F^\ell$. The set of descendants of $\{x, y\}$ is the set:

$$\mathrm{Desc}(\{x,y\}) = \{d \in F^n \mid \forall i \in \{1,2,\ldots,\ell\},\ d_i \in \{x_i, y_i\}\}.$$



Definitions

Definition

Let $C \subseteq F^\ell$. The set of descendants of C is

$$\mathrm{Desc}(C) = \bigcup_{x,y \in C} \mathrm{Desc}(\{x, y\}).$$

Definitions

Definition

Let $C \subseteq F^\ell$. The set of descendants of C is

$$\mathrm{Desc}(C) = \bigcup_{x,y \in C} \mathrm{Desc}(\{x, y\}).$$

Example

Let $C \subseteq F^\ell$ be the *repetition code* over F of length ℓ.

Definitions

Definition

Let $C \subseteq F^\ell$. The set of descendants of C is

$$\mathrm{Desc}(C) = \bigcup_{x,y \in C} \mathrm{Desc}(\{x, y\}).$$

Example

Let $C \subseteq F^\ell$ be the *repetition code* over F of length ℓ.

$\mathrm{Desc}(C)$: the set of all words involving no more than 2 distinct symbols.

Definitions

Definition

Let $C \subseteq F^{\ell}$ and let $d \in \mathrm{Desc}(C)$.

- We say that $\{x, y\} \subseteq C$ is a (possible) parent set for d if $d \in \mathrm{Desc}(\{x, y\})$.

Definitions

Definition

Let $C \subseteq F^{\ell}$ and let $d \in \mathrm{Desc}(C)$.

- We say that $\{x, y\} \subseteq C$ is a (possible) parent set for d if $d \in \mathrm{Desc}(\{x, y\})$.
- We say that d has an identifiable parent if the intersection of all parent sets of d is non-trivial.

Definitions

Example

$$C = \{{\color{red}\blacksquare\blacksquare\blacksquare}, {\color{blue}\blacksquare\blacksquare\blacksquare}, {\color{green}\blacksquare\blacksquare\blacksquare}, {\color{red}\blacksquare}{\color{blue}\blacksquare}{\color{green}\blacksquare}\} \text{ and } d = {\color{red}\blacksquare\blacksquare}{\color{green}\blacksquare}.$$

Definitions

Example

$$C = \{{\color{red}\blacksquare\blacksquare\blacksquare}, {\color{blue}\blacksquare\blacksquare\blacksquare}, {\color{green}\blacksquare\blacksquare\blacksquare}, {\color{red}\blacksquare}{\color{blue}\blacksquare}{\color{green}\blacksquare}\} \text{ and } d = {\color{red}\blacksquare\blacksquare}{\color{green}\blacksquare}.$$

Parent sets of d: $\{{\color{red}\blacksquare\blacksquare\blacksquare}, {\color{green}\blacksquare\blacksquare\blacksquare}\}$ and $\{{\color{red}\blacksquare\blacksquare\blacksquare}, {\color{red}\blacksquare}{\color{blue}\blacksquare}{\color{green}\blacksquare}\}$.

Definitions

Example

$C = \{$, , , $\}$ and $d =$ .

Parent sets of d: $\{$, $\}$ and $\{$, $\}$. So d has an identified parent (namely ).

Definitions

Example

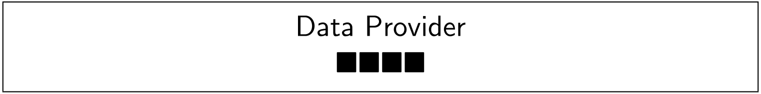
$C = \{$🟥🟥🟥, 🟦🟦🟦, 🟩🟩🟩, 🟥🟦🟩$\}$ and $d =$ 🟥🟥🟩.

Parent sets of d: $\{$🟥🟥🟥, 🟩🟩🟩$\}$ and $\{$🟥🟥🟥, 🟥🟦🟩$\}$. So d has an identified parent (namely 🟥🟥🟥).

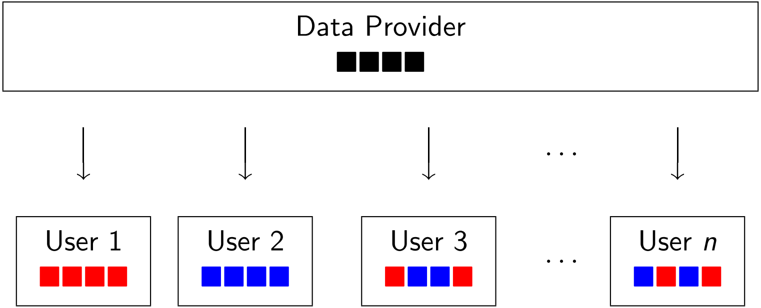
Definition

A code C has the Identifiable Parent Property (C is an IPP code) if every $d \in \mathrm{Desc}(C)$ has an identifiable parent.

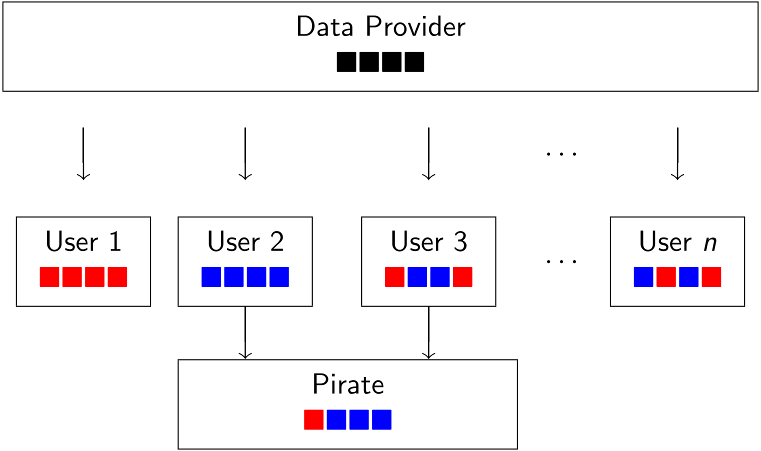
An application: copyright protection



An application: copyright protection



An application: copyright protection



Connections with error correcting codes

- If $x, y \in C$ then $|\mathrm{Desc}(\{x, y\})| = 2^{d(x,y)}$.

Connections with error correcting codes

- If $x, y \in C$ then $|\mathrm{Desc}(\{x, y\})| = 2^{d(x,y)}$.
- If C has minimum distance greater than $(3/4)\ell$, then C is an IPP code.

Connections with error correcting codes

- If $x, y \in C$ then $|\mathrm{Desc}(\{x, y\})| = 2^{d(x,y)}$.
- If C has minimum distance greater than $(3/4)\ell$, then C is an IPP code.

Question

Is there an analogue of a perfect error correcting code, for IPP codes?

Connections with error correcting codes

- If $x, y \in C$ then $|\mathrm{Desc}(\{x, y\})| = 2^{d(x,y)}$.
- If C has minimum distance greater than $(3/4)\ell$, then C is an IPP code.

Question

Is there an analogue of a perfect error correcting code, for IPP codes?

Definition

An IPP code is prolific if $\mathrm{Desc}(C) = F^{\ell}$.

Examples of prolific IPP codes

Some trivial examples

- The code F of length 1.

Examples of prolific IPP codes

Some trivial examples

- The code F of length 1.
- The repetition code of length 2.

Examples of prolific IPP codes

Some trivial examples

- The code F of length 1.
- The repetition code of length 2.
- When $q = 2$, any word and its complement.

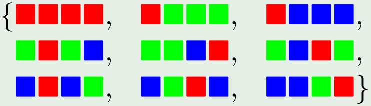
Examples of prolific IPP codes

Some trivial examples

- The code F of length 1.
- The repetition code of length 2.
- When $q = 2$, any word and its complement.

Example

The ternary Hamming code of length 4:



Bounds on the size of a prolific IPP code

Theorem

Let C be a q-ary prolific IPP code of length ℓ with m codewords. Then

$$\binom{m}{2} 2^{\ell} \geq q^{\ell}.$$

Bounds on the size of a prolific IPP code

Theorem

Let C be a q-ary prolific IPP code of length ℓ with m codewords. Then

$$\binom{m}{2} 2^{\ell} \geq q^{\ell}.$$

Theorem

(Due to Hollmann et al.) Let C be a q-ary IPP code of length ℓ with m codewords. Then

$$m \leq 3q^{\lceil \ell/3 \rceil}.$$

Non-existence results

Corollary

- *Let q be fixed, $q > 8$. There are no q-ary prolific IPP codes of length ℓ, when ℓ is sufficiently large.*

Non-existence results

Corollary

- *Let q be fixed, $q > 8$. There are no q-ary prolific IPP codes of length ℓ, when ℓ is sufficiently large.*
- *Let ℓ be fixed, $\ell > 2$. There are no q-ary prolific IPP codes of length ℓ, when q is sufficiently large.*

Non-existence results

Corollary

- *Let q be fixed, $q > 8$. There are no q-ary prolific IPP codes of length ℓ, when ℓ is sufficiently large.*
- *Let ℓ be fixed, $\ell > 2$. There are no q-ary prolific IPP codes of length ℓ, when q is sufficiently large.*

Theorem

There are no more examples of prolific IPP codes when $\ell \leq 5$.

Non-existence results

Corollary

- *Let q be fixed, $q > 8$. There are no q-ary prolific IPP codes of length ℓ, when ℓ is sufficiently large.*
- *Let ℓ be fixed, $\ell > 2$. There are no q-ary prolific IPP codes of length ℓ, when q is sufficiently large.*

Theorem

There are no more examples of prolific IPP codes when $\ell \leq 5$.

Theorem

There are no more examples of prolific IPP codes that are equivalent to linear codes.

Questions and problems

Conjecture

There are no more examples of prolific IPP codes.

Questions and problems

Conjecture

There are no more examples of prolific IPP codes.

- Can you prove there are no 3-ary examples?
- Can you prove there are no 8-ary examples?
- No examples for sufficiently large ℓ?