Password hacking, the de Bruijn way.

Dan Fretwell

Outline of talk

1. Magic...
2. de Bruijn sequences
3. Constructing de Bruijn sequences
4. Magic...explained

Magic...

Let's do a magic trick. Why not?

Magic...

Let’s do a magic trick. Why not?

Here’s a cool mind reading trick.

Magic...

Let's do a magic trick. Why not?

Here's a cool mind reading trick.

The fool giving this talk is about to ask for five volunteers.

Magic...

Let's do a magic trick. Why not?

Here's a cool mind reading trick.

The fool giving this talk is about to ask for five volunteers.

See...magic...

Proper magic...

I have a deck of cards.

Proper magic...

I have a deck of cards.

Volunteer 1, take the cards and cut the deck as many times as you want. Take the top card and pass the deck to Volunteer 2.

Proper magic...

I have a deck of cards.

Volunteer 1, take the cards and cut the deck as many times as you want. Take the top card and pass the deck to Volunteer 2.

Volunteer $n \geq 2$, take top card from deck and pass to volunteer $n+1$ until volunteer 5 has a card.

For each of the following questions put your hand up if you satisfy the criterion:

For each of the following questions put your hand up if you satisfy the criterion:

- Who has a red card?

For each of the following questions put your hand up if you satisfy the criterion:

- Who has a red card?
- Who has a surname beginning with a letter in the first half of the alphabet? (A-M)

For each of the following questions put your hand up if you satisfy the criterion:

- Who has a red card?
- Who has a surname beginning with a letter in the first half of the alphabet? (A-M)
- Who didn't cheat on last years exams?

For each of the following questions put your hand up if you satisfy the criterion:

- Who has a red card?
- Who has a surname beginning with a letter in the first half of the alphabet? (A-M)
- Who didn't cheat on last years exams?
- Who eats pickles on burgers?

For each of the following questions put your hand up if you satisfy the criterion:

- Who has a red card?
- Who has a surname beginning with a letter in the first half of the alphabet? (A-M)
- Who didn't cheat on last years exams?
- Who eats pickles on burgers?
- Who is here only because they wanted to listen to Nick's talk?

How was* I able to guess all five cards?

(* replace with wasn't if necessary.)

How was* I able to guess all five cards?

(* replace with wasn't if necessary.)

We'll find out in this talk.

Outline of talk

1 Magic...

2 de Bruijn sequences

3 Constructing de Bruijn sequences

4 Magic...explained

Question

How do you brute force a password of length n made from a finite set X of symbols?

Question

How do you brute force a password of length n made from a finite set X of symbols?

Answer

Try all $|X|^n$ possibilities!

Question

How do you brute force a password of length n made from a finite set X of symbols?

Answer

Try all $|X|^n$ possibilities!

If $|X|$ or n is large then we really don't have time for that.

But what if the machine lets you type continually until the correct password is entered?

But what if the machine lets you type continually until the correct password is entered?

Hmmm...we would need a string of symbols that contains every $\mathbf{v} \in X^n$ as a consecutive substring at least once.

But what if the machine lets you type continually until the correct password is entered?

Hmmm...we would need a string of symbols that contains every $\mathbf{v} \in X^n$ as a consecutive substring at least once.

Obviously we could just concatenate all possibilities and enter that, but this is equivalent to the previous attack. Can we do better?

Let's be efficient...there's no point entering a substring twice.

Let's be efficient...there's no point entering a substring twice.

A de Bruijn sequence of order n for X is a sequence of elements of X such that every $\mathbf{v} \in X^n$ is a consecutive substring exactly once (allowing cycling).

Let's be efficient...there's no point entering a substring twice.

A de Bruijn sequence of order n for X is a sequence of elements of X such that every $\mathbf{v} \in X^n$ is a consecutive substring exactly once (allowing cycling).

We can make some small examples easily:

Let's be efficient...there's no point entering a substring twice.

A de Bruijn sequence of order n for X is a sequence of elements of X such that every $\mathbf{v} \in X^n$ is a consecutive substring exactly once (allowing cycling).

We can make some small examples easily:

If $X = \{0, 1\}$ then the following are de Bruijn sequences of order $n = 1, 2, 3, 4$:

$$01$$

$$0011$$

$$00010111$$

$$0000100110101111$$

In a de Bruijn sequence each consecutive substring of order n has to be different and must cover all of the $|X|^n$ possibilities.

In a de Bruijn sequence each consecutive substring of order n has to be different and must cover all of the $|X|^n$ possibilities.

We have proved the following:

A de Bruijn sequence of order n for X, if it exists, has length $|X|^n$.

In a de Bruijn sequence each consecutive substring of order n has to be different and must cover all of the $|X|^n$ possibilities.

We have proved the following:

A de Bruijn sequence of order n for X, if it exists, has length $|X|^n$.

Note that this is much smaller than $n|X|^n$, the size of the string needed to break the password the old fashioned way!

Outline of talk

1 Magic...

2 de Bruijn sequences

3 Constructing de Bruijn sequences

4 Magic...explained

The following is non-trivial!

Theorem

If X is a finite set and $n \geq 1$ then there exists a de Bruijn sequence of order n for X.

In fact, if $k = |X|$ then there are $\frac{(k!)^{k^{(n-1)}}}{k^n}$ of them.

The following is non-trivial!

Theorem

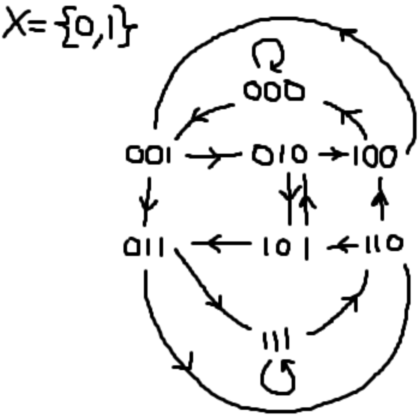
If X is a finite set and $n \geq 1$ then there exists a de Bruijn sequence of order n for X.

In fact, if $k = |X|$ then there are $\frac{(k!)^{k^{(n-1)}}}{k^n}$ of them.

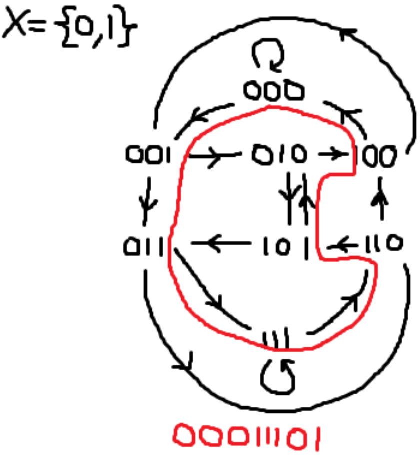
Question

How do we make one?

We can make de Bruijn sequences by finding Hamiltonian paths in certain graphs.



We can make de Bruijn sequences by finding Hamiltonian paths in certain graphs.



In the case where $X = \mathbb{Z}/p\mathbb{Z}$ we can construct de Bruijn sequences recursively.

Let $f(t) = t^n + A_{n-1}t^{n-1} + \ldots + A_1 t + A_0 \in (\mathbb{Z}/p\mathbb{Z})[t]$ be irreducible. Then the recursion:

$$x_{m+n} \equiv A_{n-1}x_{m+n-1} + \ldots + A_1 x_{m+1} + A_0 x_m \bmod p$$

gives a de Bruijn sequence of order n for any non-zero initial vector $\mathbf{v} = (x_0, x_1, \ldots, x_{n-1}) \in (\mathbb{Z}/p\mathbb{Z})^n$.

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

$$001$$

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

0010

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

00101

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

001011

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

$$0010111$$

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

$$00101110$$

Example

If $p = 2$ then $t^3 + t + 1$ is an irreducible polynomial of degree 3 over $\mathbb{Z}/2\mathbb{Z}$.

Starting with seed 001 we get the sequence:

$$00101110$$

Outline of talk

1. Magic...
2. de Bruijn sequences
3. Constructing de Bruijn sequences
4. Magic...explained

So how did the magic trick work? It should be clear that only the red card question was relevant.

So how did the magic trick work? It should be clear that only the red card question was relevant.

But surely that isn't enough information...there are only $2^5 = 32$ possible answers to that question but many more possible 5-tuples of cards.

So how did the magic trick work? It should be clear that only the red card question was relevant.

But surely that isn't enough information...there are only $2^5 = 32$ possible answers to that question but many more possible 5-tuples of cards.

Confession 1

The deck contained only 32 cards, the ones with numerical value up to 8.

So how did the magic trick work? It should be clear that only the red card question was relevant.

But surely that isn't enough information...there are only $2^5 = 32$ possible answers to that question but many more possible 5-tuples of cards.

Confession 1

The deck contained only 32 cards, the ones with numerical value up to 8.

Confession 2

The deck was rigged!

We can encode the cards in our deck as binary strings of length 5, two bits for the suit and three for the number:

$$\text{Clubs} \to 00 \qquad \text{Spades} \to 01$$
$$\text{Diamonds} \to 10 \qquad \text{Hearts} \to 11$$

$$\begin{array}{ll} A \to 001 & 5 \to 101 \\ 2 \to 010 & 6 \to 110 \\ 3 \to 011 & 7 \to 111 \\ 4 \to 100 & 8 \to 000 \end{array}$$

For example:

$5H \to 11101$ AC 00001 $8S \to 01000$

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

00001001011001111100011011101010

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

00001001011001111100011011101010

I can use this to set up a deck:

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

00001001011001111100011011101010

I can use this to set up a deck:

AC

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

$$0\textcolor{red}{00010}01011001111100011011101010$$

I can use this to set up a deck:

$$\mathrm{AC}, \textcolor{red}{2\mathrm{C}}$$

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

00000100101100111110001101110101 0

I can use this to set up a deck:

$\mathrm{AC}, 2\mathrm{C}, 4\mathrm{C}$

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

$$00001001011001111100011011101010$$

I can use this to set up a deck:

$$\text{AC}, \text{2C}, \text{4C}, \text{AS}$$

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

$$\color{red}{0000}\color{black}{100101100111110001101110101}\color{red}{0}$$

I can use this to set up a deck:

$$\text{AC}, \text{2C}, \text{4C}, \text{AS}, \ldots, \color{red}{\text{8C}}$$

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

00000100101100111110001101110101 0

I can use this to set up a deck:

AC, 2C, 4C, AS, ..., 8C

Cutting the deck corresponds to cycling the sequence...which doesn't change the de Bruijn property.

Here is a de Bruijn sequence of order 5 for $X = \{0, 1\}$:

$$00001001011001111100011011101010$$

I can use this to set up a deck:

$$\text{AC}, \text{2C}, \text{4C}, \text{AS}, \ldots, \text{8C}$$

Cutting the deck corresponds to cycling the sequence...which doesn't change the de Bruijn property.

Note that the 1's in the sequence translate into red cards. So knowing who has a red card gives a binary sequence of length 5 corresponding to what the first card drawn was!

How did I know the other four cards?

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards! For example:

$$01011$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \mod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$010110 \to 010110$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$0101100 \rightarrow 0101100$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$01011001 \rightarrow 01011001$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \mod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$010110011 \rightarrow 010110011$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$010110011 \to 3S$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \mod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$0\textcolor{red}{10110}011 \to 3S, \textcolor{red}{6D}$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$01{\color{red}01100}11 \rightarrow 3S, 6D, {\color{red}4S}$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \mod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$010110011 \rightarrow 3S, 6D, 4S, AH$$

How did I know the other four cards?

The de Bruijn sequence (x_n) in the previous slide is generated by the recursion $x_{n+5} \equiv x_n + x_{n+2} \bmod 2$ (with $\mathbf{v} = 00001$).

So once I know what the first card drawn was, I can generate the binary sequences corresponding to the next four cards!

For example:

$$010\mathbf{\color{red}{10011}} \rightarrow 3S, 6D, 4S, AH, {\color{red}3D}$$

Thanks for listening