Consecutive Switch Codes for Network Switches

Sarit Buzaglo\textsuperscript{1}, Eitan Yaakobi\textsuperscript{2}, Yuval Cassuto\textsuperscript{2}, and Paul H. Siegel\textsuperscript{1}

\textsuperscript{1}CMRR

\textsuperscript{2}Technion

Coding Theory Seminar
July 3, 2016
Outline

- Introduction
- Construction of binary switch codes.
- Consecutive switch codes.
- Conclusion
Network switches

A network switch consists of $n$ input ports, $k$ output ports, and $m$ banks.

In each time slot, called generation $n$ input packets are processed and stored in the banks. A read controller outputs any request of $k$ packets by accessing at most one packet from every bank.
Switch codes

Switch codes are coding schemes that are designed to read and write data in network switches. A \((n, k, m)_q\)-switch code is defined as follows.

1) For every \(T \geq 1\), a vector \(x^{(T)} \in \mathbb{F}_q^n\) is encoded to a vector \(c^{(T)} \in \mathbb{F}_q^m\).

2) For every request set of \(k\) packets \(I = \{x^{(T_1)}_{i_1}, x^{(T_2)}_{i_2}, \ldots, x^{(T_k)}_{i_k}\}\), there exist \(k\) disjoint recovery sets \(J_1, J_2, \ldots, J_k \subset [m]\) such that for every \(1 \leq r \leq k\), the packet \(x^{(T_r)}_{i_r}\) can be recovered from \(\{c^{(T_r)}_j\}_{j \in J_r}\). We call \(\{c^{(T_r)}_j\}_{j \in J_r}\) the recovery subsequence for \(x^{(T_r)}_{i_r}\).
Switch codes

Example

A \((n = 2, k = 2, m = 3)\) binary switch code
Switch codes

Example

A \((n = 2, k = 2, m = 3)\) binary switch code
Switch codes

Example
A \((n = 2, k = 2, m = 3)\) binary switch code

\[
\begin{align*}
&x_1^{(1)} \oplus x_2^{(1)} = x_1^{(T)} \oplus x_2^{(T)} \\
&x_1^{(2)} \oplus x_2^{(2)} = x_1^{(2)} \oplus x_2^{(2)} \\
&x_1^{(1)} \oplus x_2^{(1)} = x_1^{(1)} \oplus x_2^{(1)}
\end{align*}
\]
Switch codes

In this talk we consider only the case $n = k$ and refer to switch codes as $(n, m)_q$-switch codes. In particular we are interested in binary codes.
Switch codes

In this talk we consider only the case $n = k$ and refer to switch codes as $(n, m)_q$-switch codes. In particular we are interested in binary codes.

Related work

- Wang et al., 2013- Presented switch codes, constructions, and bounds in terms of the degree.
- Wang et al., 2015- Construction of binary switch code with $m = n^2 / \log_2 n$.
- Ishai et al., 2004- Presented and constructed batch codes. A construction of a binary switch code with $m = n^{\log_2 3} > n^{1.5849}$. 


Switch codes

In this talk we consider only the case $n = k$ and refer to switch codes as $(n, m)_q$-switch codes. In particular we are interested in binary codes.

Related work

- Wang et al., 2013- Presented switch codes, constructions, and bounds in terms of the degree.
- Wang et al., 2015- Construction of binary switch code with $m = n^2 / \log_2 n$.
- Ishai et al., 2004- Presented and constructed batch codes. A construction of a binary switch code with $m = n^{\log_2 3} > n^{1.5849}$.

We will show a construction of binary switch code with $m \approx 2n^{1.5}$. 
Construction of switch code

A \((\nu, n)\)-one-step majority code with availability \(s\) is a code, \(C\), that encodes \(x \in \mathbb{F}_q^n\) to \(\mathcal{E}(x) \in \mathbb{F}_q^{(\nu)}\) and for all \(i \in [n]\), there exist \(s\) disjoint subsets \(J_1, J_2, \ldots, J_s \subset [\nu]\), such that for every \(1 \leq r \leq s\), the packet \(x_i\) can be recovered from \(\{\mathcal{E}(x)_j\}_{j \in J_r}\).
Construction of switch code

A \((\nu, n)\)-one-step majority code with availability \(s\) is a code, \(C\), that encodes \(x \in \mathbb{F}_q^n\) to \(E(x) \in \mathbb{F}_q^{(\nu)}\) and for all \(i \in [n]\), there exist \(s\) disjoint subsets \(J_1, J_2, \ldots, J_s \subset [\nu]\), such that for every \(1 \leq r \leq s\), the packet \(x_i\) can be recovered from \(\{E(x)_j\}_{j \in J_r}\).

Theorem

If \(C\) is a \((\nu, n)\)-one-step majority code over \(\mathbb{F}_q\) with availability \(s\), where \(s \leq n\), then the code that maps \(x\) to

\[
c = x | x | \cdots | x | E(x) | E(x) | \cdots | E(x) \underbrace{}_{s \text{ times}} \underbrace{}_{\lceil n/s \rceil \text{ times}}
\]

is a \((n, m)_q\)-switch code, with \(m = sn + \lceil n/s \rceil \nu\).
Proof.

- It is sufficient to show that for any multi-set \( I = \{ i_1, i_2, \ldots, i_n \} \) of \( n \) indices, the information symbols \( x_{i_1}, x_{i_2}, \ldots, x_{i_n} \) can be recovered from \( n \) disjoint recovery subsequences of \( c \).
Proof.

• It is suffice to show that for any multi-set \( I = \{i_1, i_2, \ldots, i_n\} \) of \( n \) indices, the information symbols \( x_{i_1}, x_{i_2}, \ldots, x_{i_n} \) can be recovered from \( n \) disjoint recovery subsequences of \( c \).

• For every \( 1 \leq i \leq n \), let \( r_i \) be the number of appearances of \( i \) in the multi-set \( I \) and let \( m_i = \min\{s, r_i\} \). Hence,

\[
\sum_{i=1}^{n} r_i = n.
\]
Proof.

• It is suffice to show that for any multi-set \( I = \{i_1, i_2, \ldots, i_n\} \) of \( n \) indices, the information symbols \( x_{i_1}, x_{i_2}, \ldots, x_{i_n} \) can be recovered from \( n \) disjoint recovery subsequences of \( c \).

• For every \( 1 \leq i \leq n \), let \( r_i \) be the number of appearances of \( i \) in the multi-set \( I \) and let \( m_i = \min\{s, r_i\} \). Hence,

\[
\sum_{i=1}^{n} r_i = n.
\]

• Since \( m_i \leq s \), we can recover \( m_i \) copies of \( x_i \) directly from the \( s \) copies of \( x \).
• To recover the remaining $r_i - m_i$ copies of $x_i$ we first find $s$ disjoint subsequences of $z = \mathcal{E}(x)$ that can each recover $x_i$. Then, we use at most $\left\lceil \frac{r_i - m_i}{s} \right\rceil \leq \frac{r_i}{s}$ copies of each of the $s$ subsequences to recover $x_i$. 
Proof Continues

- To recover the remaining $r_i - m_i$ copies of $x_i$ we first find $s$ disjoint subsequences of $z = \mathcal{E}(x)$ that can each recover $x_i$. Then, we use at most $\left\lceil \frac{r_i - m_i}{s} \right\rceil \leq \frac{r_i}{s}$ copies of each of the $s$ subsequences to recover $x_i$.

- For every $1 \leq j \leq \nu$ and for every $1 \leq i \leq n$ we used at most $\frac{r_i}{s}$ copies of $z_j$ to recover $x_i$. Hence, we used at most

$$\left\lfloor \left\lceil \frac{n}{s} \right\rceil \right\rfloor \leq \frac{n}{s}$$

copies of $z_j$ and indeed $c$ consists of enough copies of $z$. 
Lemma (Lin and Costello, 2004, p. 293)

The binary cyclic 
$(\nu = 2^{2r} + 2^r + 1, n = 2^{2r} + 2^r - 3^r)$-difference-set code is a binary 
$(\nu, n)$-one-step majority code with availability $s = 2^r + 1 \approx \sqrt{n}$. 
Lemma (Lin and Costello, 2004, p. 293)

The binary cyclic
\( (\nu = 2^{2r} + 2^r + 1, n = 2^{2r} + 2^r - 3^r) \)-difference-set code is a binary
\((\nu, n)\)-one-step majority code with availability \( s = 2^r + 1 \approx \sqrt{n} \).

Corollary

There exists an (explicit) \((n, m)_{2}\)-switch code, with

\[
m = sn + \left\lfloor \frac{n}{s} \right\rfloor \nu \approx 2n^{1.5}.
\]
Consecutive switch codes

A \textbf{ℓ-consecutive switch code} is a switch code in which the request sets are restricted to \( \ell \) consecutive generations, i.e., of the form

\[
I = \{ x_{i_1}^{(T_1)}, x_{i_2}^{(T_2)}, \ldots, x_{i_k}^{(T_k)} \}
\]

and

\[
T_1, T_2, \ldots, T_k \in \{ T, T + 1, T + 2, \ldots, T + \ell - 1 \}.
\]
Consecutive switch codes

A \( \ell \)-consecutive switch code is a switch code in which the request sets are restricted to \( \ell \) consecutive generations, i.e., of the form

\[
I = \{x_{i_1}^{(T_1)}, x_{i_2}^{(T_2)}, \ldots, x_{i_k}^{(T_k)}\}
\]

and

\[
T_1, T_2, \ldots, T_k \in \{T, T + 1, T + 2, \ldots, T + \ell - 1\}.
\]

**Advantage:** Admit better rates \((n/m)\) and yet deliver a large collection of common request sets.
Consecutive switch codes

Example

A \((n = 4, k = 4, m = 6)\)\(2\)-\(\ell\)-consecutive switch code with \(\ell = 2\).

\[
\begin{array}{cccccc}
\text{1st Line} \\
\hline
x_1^{(2)} & x_2^{(2)} & x_3^{(2)} & x_4^{(2)} & x_3^{(2)} \oplus x_4^{(2)} & x_1^{(2)} \oplus x_2^{(2)} \\
\end{array}
\]

\[
\begin{array}{cccccc}
\text{2nd Line} \\
\hline
x_1^{(1)} & x_2^{(1)} & x_3^{(1)} & x_4^{(1)} & x_1^{(1)} \oplus x_2^{(1)} & x_3^{(1)} \oplus x_4^{(1)} \\
\end{array}
\]

\[
\begin{array}{cccccc}
\text{3rd Line} \\
\hline
12 / 21 \\
\end{array}
\]
Consecutive switch codes

Example

A \((n = 4, k = 4, m = 6)_{2-\ell}\)-consecutive switch code with \(\ell = 2\).

\[
\begin{array}{cccccc}
  x_1^{(2)} & x_2^{(2)} & x_3^{(2)} & x_4^{(2)} & x_3^{(2)} \oplus x_4^{(2)} & x_1^{(2)} \oplus x_2^{(2)} \\
  x_1^{(1)} & x_2^{(1)} & x_3^{(1)} & x_4^{(1)} & x_1^{(1)} \oplus x_2^{(1)} & x_3^{(1)} \oplus x_4^{(1)}
\end{array}
\]
Consecutive switch codes

Example

A \((n = 4, k = 4, m = 6)_{2-\ell}\)-consecutive switch code with \(\ell = 2\).
Combinatorial switch code

In a **combinatorial** switch code, the entries of a codeword $c^T$ are simply copies of the entries of the input vector $x^T$.

A combinatorial $\ell$-consecutive switch code can be represented by a matrix $F \in [n]^{\ell \times m}$. 

Combinatorial switch code

In a **combinatorial** switch code, the entries of a codeword $c^T$ are simply copies of the entries of the input vector $x^T$.

A combinatorial $\ell$-consecutive switch code can be represented by a matrix $F \in [n]^{\ell \times m}$.

**Example**

A combinatorial $(n = 3, k = 3, m = 5)$-2-consecutive switch code

$$F = \begin{pmatrix} 1 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 \end{pmatrix} \in [3]^{2 \times 5}$$
Combinatorial switch codes for $\ell = 2$

Henceforth, we will focus only on combinatorial consecutive switch codes and the case $k = n$. We refer to combinatorial consecutive switch codes as $(n, m)$-switch codes.

**Theorem**

For every $(n, m)$-2-switch code we have $m \geq 2n - 1$.

**Remark:** The $\ell$-repetition code, formed by repeating each input symbol $\ell$-times, is a $(n, m)$-$\ell$-switch code with $m = \ell n$.

Q: Can we construct a $(n, m)$-2-switch code with $m = 2n - 1$?

Yes.

$F = (1 \ 2 \ \cdots \ n \ n \ n \ \cdots \ n \ 1 \ 2 \ \cdots \ n \ 1 \ 2 \ \cdots \ n - 1)$
Combinatorial switch codes for $\ell = 2$

Henceforth, we will focus only on combinatorial consecutive switch codes and the case $k = n$. We refer to combinatorial consecutive switch codes as $(n, m)$-$\ell$-switch codes.

**Theorem**

*For every $(n, m)$-2-switch code we have $m \geq 2n - 1$.***
Combinatorial switch codes for $\ell = 2$

Henceforth, we will focus only on combinatorial consecutive switch codes and the case $k = n$. We refer to combinatorial consecutive switch codes as $(n, m)$-$\ell$-switch codes.

**Theorem**

For every $(n, m)$-2-switch code we have $m \geq 2n - 1$.

**Remark:** The $\ell$-repetition code, formed by repeating each input symbol $\ell$-times, is a $(n, m)$-$\ell$-switch code with $m = \ell n$. 
Combinatorial switch codes for $\ell = 2$

Henceforth, we will focus only on combinatorial consecutive switch codes and the case $k = n$. We refer to combinatorial consecutive switch codes as $(n, m)$-$\ell$-switch codes.

**Theorem**

For every $(n, m)$-2-switch code we have $m \geq 2n - 1$.

**Remark:** The $\ell$-repetition code, formed by repeating each input symbol $\ell$-times, is a $(n, m)$-$\ell$-switch code with $m = \ell n$.

**Q:** Can we construct a $(n, m)$-2-switch code with $m = 2n - 1$?
Combinatorial switch codes for $\ell = 2$

Henceforth, we will focus only on combinatorial consecutive switch codes and the case $k = n$. We refer to combinatorial consecutive switch codes as $(n, m)$-$\ell$-switch codes.

**Theorem**

*For every $(n, m)$-$2$-switch code we have $m \geq 2n - 1$.**

**Remark:** The $\ell$-repetition code, formed by repeating each input symbol $\ell$-times, is a $(n, m)$-$\ell$-switch code with $m = \ell n$.

**Q:** Can we construct a $(n, m)$-$2$-switch code with $m = 2n - 1$? Yes.

$$F = \begin{pmatrix} 1 & 2 & \cdots & n & n & n & \cdots & n \\ 1 & 2 & \cdots & n & 1 & 2 & \cdots & n - 1 \end{pmatrix}$$
Example

For $n = 4$ and $m = 6$:

$$F = \begin{pmatrix}
4 & 3 & 1 & 2 & 3 & 4 \\
1 & 4 & 3 & 3 & 1 & 2
\end{pmatrix}$$
Example

For \( n = 4 \) and \( m = 6 \):

\[
F = \begin{pmatrix}
4 & 3 & 1 & 2 & 3 & 4 \\
1 & 4 & 3 & 3 & 1 & 2
\end{pmatrix}
\]
Construction of a \((n, m)\)-3-switch code

We construct a combinatorial \((n, m)\)-3-switch code of the following form

\[
F = (F_1 \mid F_2 \mid F_3),
\]

where

\[
F_1 = \begin{pmatrix}
1 & 2 & \cdots & n \\
1 & 2 & \cdots & n \\
1 & 2 & \cdots & n
\end{pmatrix},
\]

\(F_2 \in [n]^{3 \times \nu}\), and \(F_3 \in [n]^{3 \times \nu}\) is obtained by a cyclic shift of the rows of \(F_2\).
Construction of a \((n, m)\)-3-switch code

We construct a combinatorial \((n, m)\)-3-switch code of the following form

\[ F = (F_1 \mid F_2 \mid F_3), \]

where

\[ F_1 = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}, \]

\[ F_2 \in [n]^{3 \times \nu}, \text{ and } F_3 \in [n]^{3 \times \nu} \]

is obtained by a cyclic shift of the rows of \(F_2\).

**Lemma**

*If every \(i_1, i_2, \ldots, i_s \in [n], s \leq n/2, \) can be found in \(s\) distinct columns of \(F_2\) then \(F\) is a \((n, m)\)-3-switch code with \(m = n + 2\nu\).*
Constructing $F_2$

Let $n = \alpha(\alpha + 1)$. $F_2 \in [n]^{3 \times \nu}$, $\nu = n - \alpha$, is of the form

$$F_2 = (A_1 \mid A_2 \mid \cdots \mid A_\alpha),$$

where

$$A_r = \begin{pmatrix} r\alpha + 2 & r\alpha + 3 & \cdots & (r + 1)\alpha & r\alpha + 1 \\ r\alpha + 1 & r\alpha + 2 & \cdots & r\alpha + \alpha - 1 & (r + 1)\alpha \\ 1 & 2 & \cdots & \alpha - 1 & \alpha \end{pmatrix},$$

$$1 \leq r \leq \alpha.$$
Constructing $F_2$

Let $n = \alpha(\alpha + 1)$. $F_2 \in [n]^{3 \times \nu}$, $\nu = n - \alpha$, is of the form

$$F_2 = (A_1 \mid A_2 \mid \cdots \mid A_\alpha),$$

where

$$A_r = \begin{pmatrix}
 r\alpha + 2 & r\alpha + 3 & \cdots & (r + 1)\alpha & r\alpha + 1 \\
 r\alpha + 1 & r\alpha + 2 & \cdots & r\alpha + \alpha - 1 & (r + 1)\alpha \\
 1 & 2 & \cdots & \alpha - 1 & \alpha
\end{pmatrix},$$

$1 \leq r \leq \alpha$.

Lemma

Every $i_1, i_2, \ldots, i_s \in [n]$, $s \leq n/2$, can be found in $s$ distinct columns of $F_2$. 

Corollary

$F$ is a $(n, m)$-3-switch code with $n = \alpha(\alpha + 1)$ and $m = 3n - 2\alpha \approx 3n - 2\sqrt{n}$. 

Constructing $F_2$

Let $n = \alpha(\alpha + 1)$. $F_2 \in [n]^{3 \times \nu}$, $\nu = n - \alpha$, is of the form

$$F_2 = (A_1 \mid A_2 \mid \cdots \mid A_\alpha),$$

where

$$A_r = \begin{pmatrix}
    r\alpha + 2 & r\alpha + 3 & \cdots & (r + 1)\alpha & r\alpha + 1 \\
    r\alpha + 1 & r\alpha + 2 & \cdots & r\alpha + \alpha - 1 & (r + 1)\alpha \\
    1 & 2 & \cdots & \alpha - 1 & \alpha
\end{pmatrix},$$

$1 \leq r \leq \alpha$.

Lemma

Every $i_1, i_2, \ldots, i_s \in [n]$, $s \leq n/2$, can be found in $s$ distinct columns of $F_2$

Corollary

$F$ is a $(n, m)$-3-switch code with $n = \alpha(\alpha + 1)$ and $m = 3n - 2\alpha \approx 3n - 2\sqrt{n}$. 
Combinatorial \((n, m)\)-3-switch code

**Example**

Let \(n = 6\), then \(\alpha = 2\),

\[
F_2 = (A_1|A_2) = \begin{pmatrix}
4 & 3 & 6 & 5 \\
3 & 4 & 5 & 6 \\
1 & 2 & 1 & 2
\end{pmatrix},
\]

and

\[
F = (F_1|F_2|F_3) = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 4 & 3 & 6 & 5 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 \\
1 & 2 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 & 4 & 3 & 6 & 5
\end{pmatrix}.
\]
Combinatorial \((n, m)\)-3-switch code

**Example**

Let \(n = 6\), then \(\alpha = 2\),

\[
F_2 = (A_1 | A_2) = \begin{pmatrix}
4 & 3 & 6 & 5 \\
3 & 4 & 5 & 6 \\
1 & 2 & 1 & 2
\end{pmatrix},
\]

and

\[
F = (F_1 | F_2 | F_3) = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 4 & 3 & 6 & 5 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 \\
1 & 2 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 & 4 & 3 & 6 & 5
\end{pmatrix}.
\]
Combinatorial \((n, m)\)-3-switch code

**Example**

Let \(n = 6\), then \(\alpha = 2\),

\[
F_2 = (A_1|A_2) = \begin{pmatrix}
4 & 3 & 6 & 5 \\
3 & 4 & 5 & 6 \\
1 & 2 & 1 & 2
\end{pmatrix},
\]

and

\[
F = (F_1|F_2|F_3) = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 4 & 3 & 6 & 5 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 \\
1 & 2 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 & 4 & 3 & 6 & 5
\end{pmatrix}.
\]
Combinatorial \((n, m)\)-3-switch code

Example
Let \(n = 6\), then \(\alpha = 2\),

\[
F_2 = (A_1|A_2) = \begin{pmatrix}
4 & 3 & 6 & 5 \\
3 & 4 & 5 & 6 \\
1 & 2 & 1 & 2
\end{pmatrix},
\]

and

\[
F = (F_1|F_2|F_3) = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 4 & 3 & 6 & 5 & 3 & 4 & 5 & 6 \\
1 & 2 & 3 & 4 & 5 & 6 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 \\
1 & 2 & 3 & 4 & 5 & 6 & 1 & 2 & 1 & 2 & 4 & 3 & 6 & 5
\end{pmatrix}.
\]
The construction is generalized for every $\ell \geq 3$

**Theorem**

If $n = (\ell - 2)\alpha^2 + (\ell - 2)\alpha$ then there exists an (explicit) $(n, m)$-$\ell$-switch code with

$m = \ell n - (\ell - 1)(\ell - 2)\alpha \approx \ell n - (\ell - 1)\sqrt{(\ell - 2)n}$. 

Conclusion

- We constructed the best known binary switch code for the case $n = k$.
- We presented consecutive switch codes, which can achieve better rates and yet recover a common type of request sets.
- We showed the tight lower bound $m = 2n - 1$ for combinatorial 2-consecutive switch codes.
- We constructed combinatorial $\ell$-consecutive switch codes, with $m \approx \ell n - (\ell - 1) \sqrt{(\ell - 2)n}$.
Open Problems

- Find lower bounds on \( m \) for switch codes/combinatorial consecutive switch codes/consectutive switch codes.
- Construct combinatorial consecutive switch codes where \( \ell \) is not fixed.
- Construct consecutive switch codes in the computational (not combinatorial) case.
Open Problems

- Find lower bounds on $m$ for switch codes/combinatorial consecutive switch codes/consectutive switch codes.
- Construct combinatorial consecutive switch codes where $\ell$ is not fixed.
- Construct consecutive switch codes in the computational (not combinatorial) case.

Thank You!