Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

магістерська дипломна робота
за напрямом 123 – «Комп'ютерна інженерія»

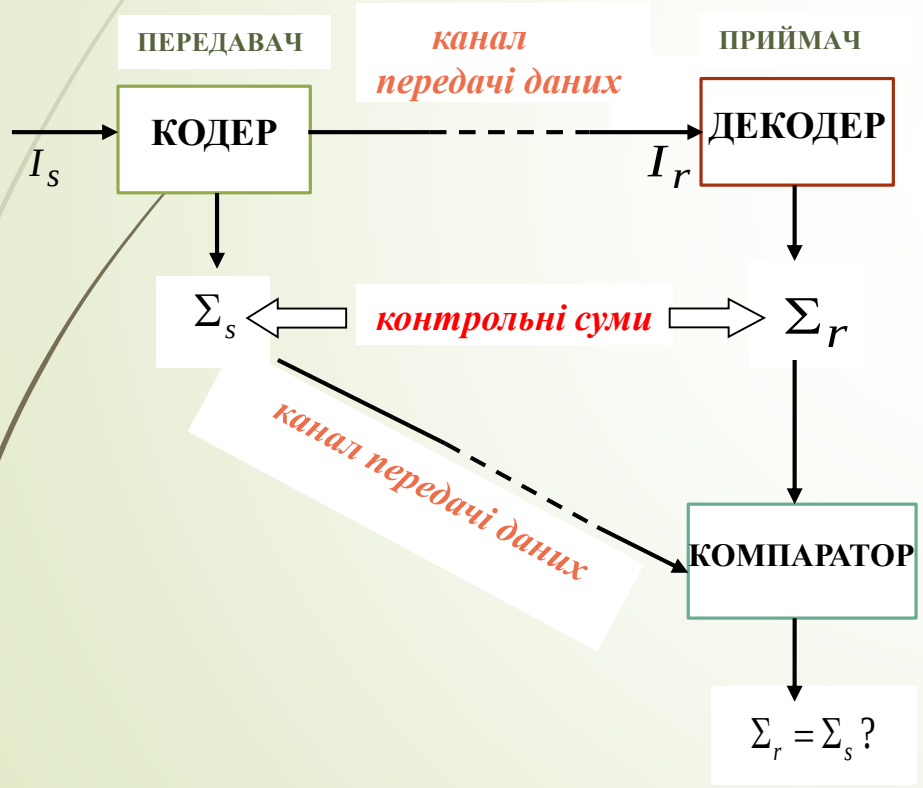
ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ПАРАЛЕЛЬНОГО ОБЧИСЛЕННЯ CRC-КОДІВ В СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

Керівник: к.т.н., доц.
Семеренко В.П.
Розробив: студент гр. 1КІ-16м
Григорчук Б.О.

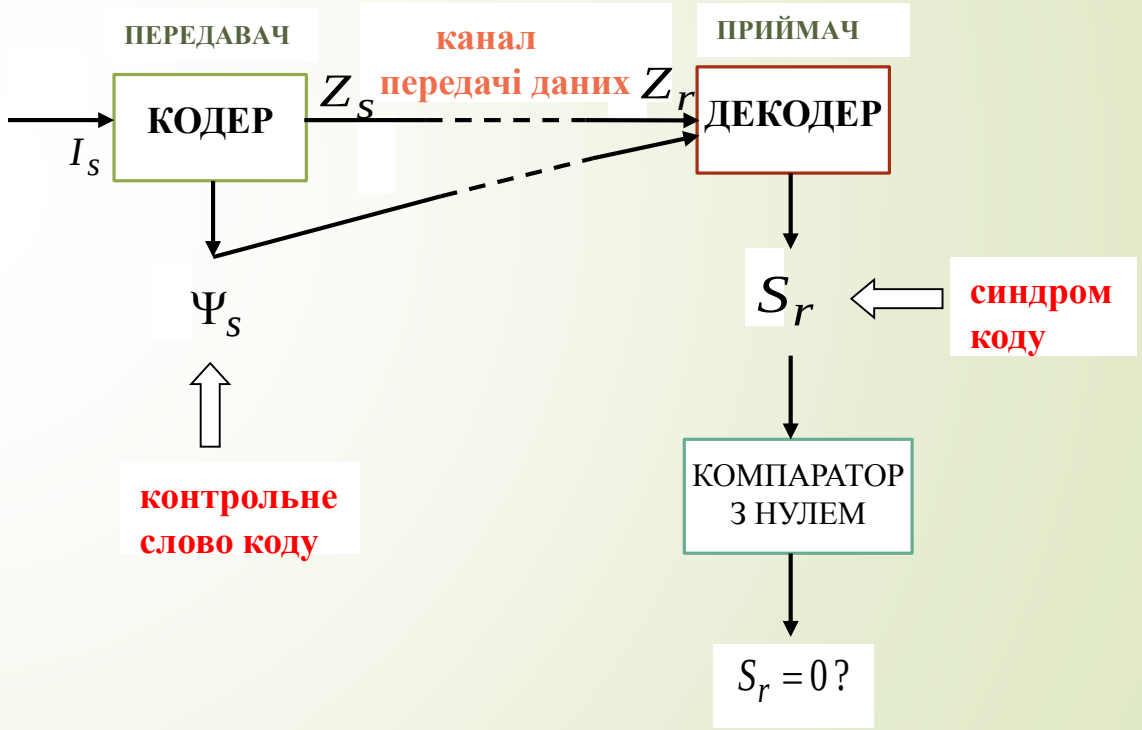
Вінниця ВНТУ 2018 р.

Абревіатура CRC має дві розшифровки, які вказують на два напрямки CRC-контролю:

- Cyclic redundancy check – циклічний надлишковий контроль (контрольна сума).



- Cyclic redundancy code – циклічний надлишковий код (циклічний код).

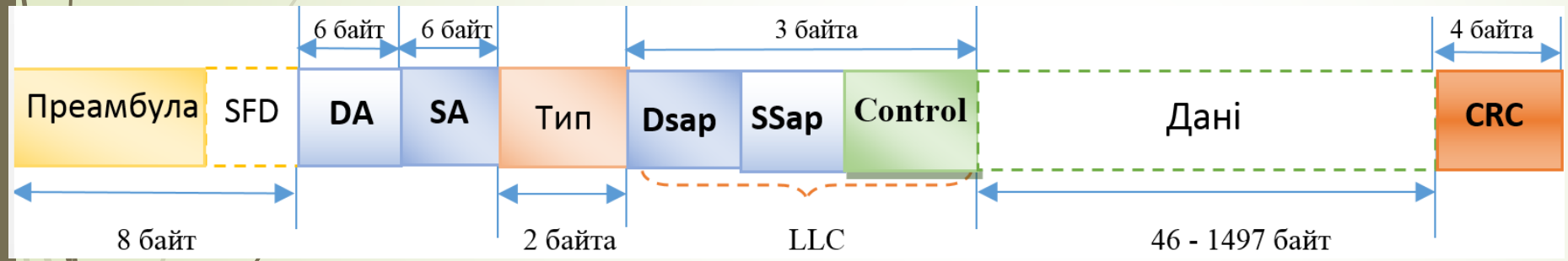


Для оптимального підбору CRC під потреби системи передачі даних, використовують поліноми

Назва CRC	Поліном
CRC-5-USB	X^5+X^2+1 - (*USB*)
CRC-7	X^7+X^3+1 - (системи телекомунікації, *ITU-T G.707*, *ITU-T G.832*, *SD*)
CRC-11	$X^{11}+X^9+X^8+X^7+X^2+1$ (*FlexRay* – високошвидкісний мережевий протокол для автомобілів)
CRC-16-IBM	$X^{16}+X^{15}+X^2+1$ (комунікаційний протокол *Modbus*; *USB*)
CRC-16-CCITT	$X^{16}+X^{12}+X^5+1$ (стандарт канального рівня мережевої моделі *OSI - X.25*; протокол *OSI - HDLC*; Протокол сайтів - *XMODEM*; *Bluetooth*; карта пам'яті *SD*)
CRC-16-T10-DIF	$X^{16}+X^{15}+X^{11}+X^9+X^8+X^7+X^5+X^4+X^2+X+1$ (*SCSI DIF* – стандарт для фізичного підключення і передачі даних між комп'ютерами і периферійними пристроями)
CRC-32-IEEE 802.3	$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$ (*V.42* - Протокол виявлення і корекції помилок для передачі даних з високими швидкостями., *MPEG-2-* стандарт цифрового кодування відео; *PNG* - растровий формат зберігання графічної інформації; *POSIX cksum* - переносний інтерфейс операційних систем)
CRC-32Q	$X^{32}+X^{31}+X^{24}+X^{22}+X^{16}+X^{14}+X^8+X^7+X^5+X^3+X+1$ (авіація; *AIXM* - модель обміну аеронавігаційною інформацією)
CRC-32	$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$ (WinRAR, ZIP, Ethernet)

Формати кадрів в мережі Ethernet

- Ethernet DIX (II)

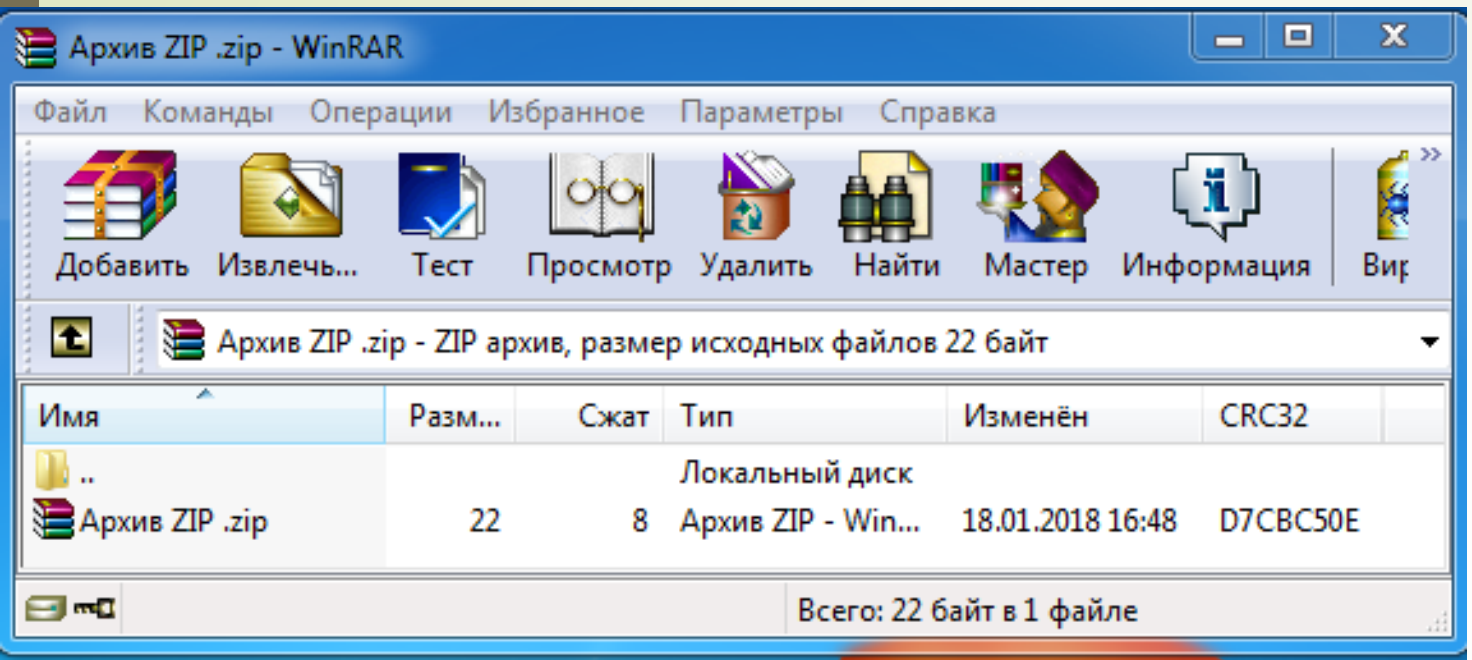


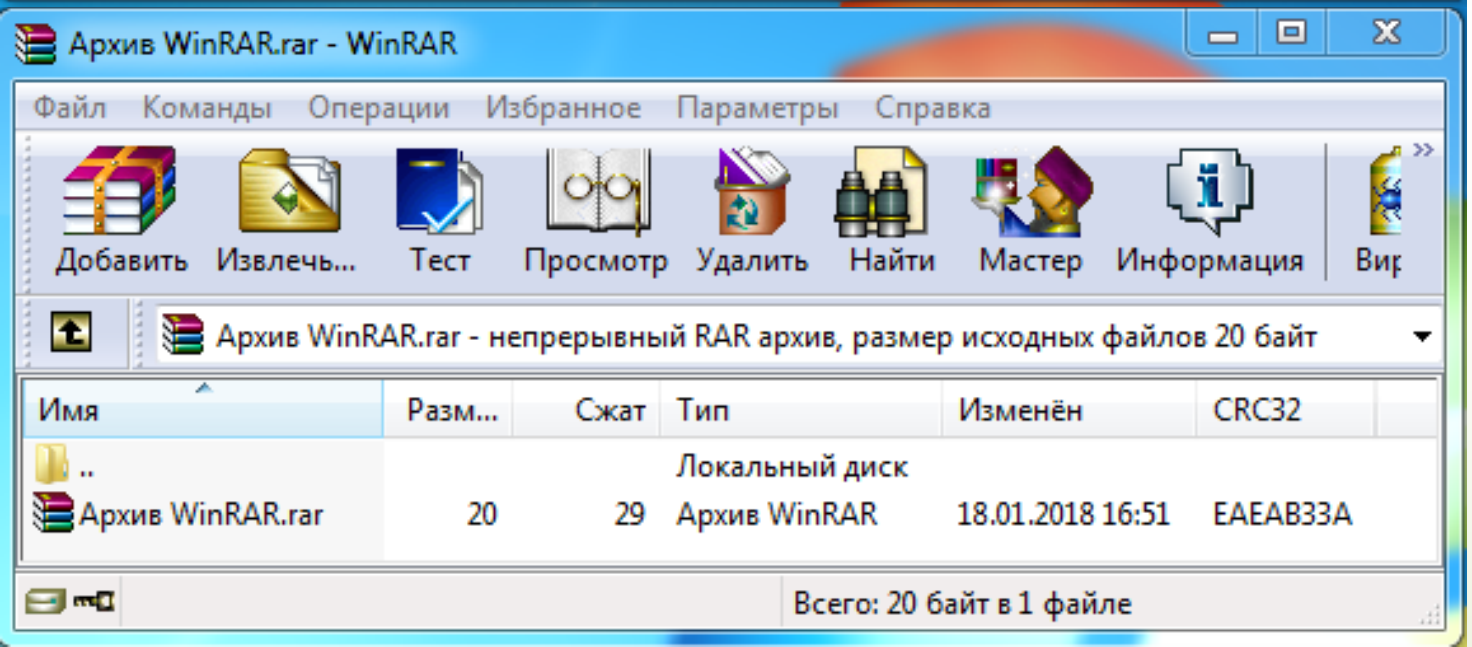
- 802.3/LLC

- Raw 802.3/Novell 802

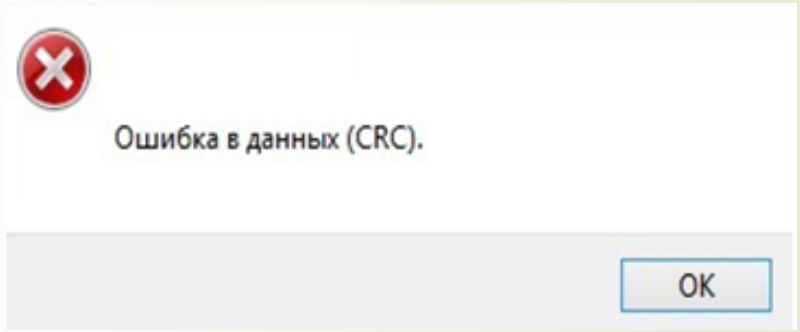
- Ethernet SNAP

CRC перевірка цілісності даних в архіваторах (Zip, Rar)

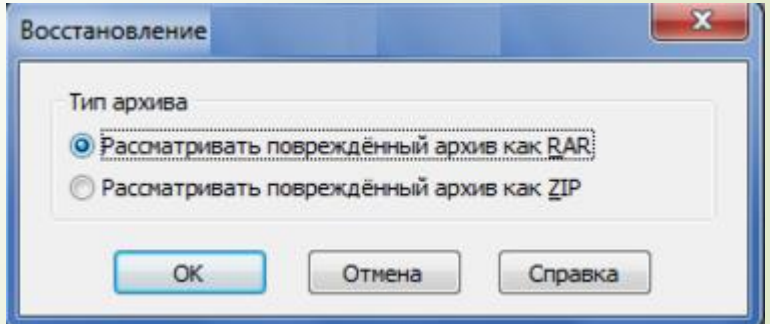




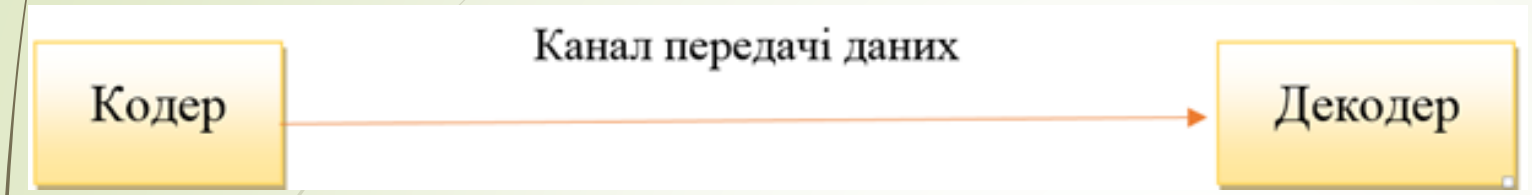
- ZIP-архіві міститься спеціальне CRC-32 поле,.. При розпаковці даних з архіву, архіватор розраховує обчислену контрольну суму, і якщо вона не збігається, то дані вважаються пошкодженими.

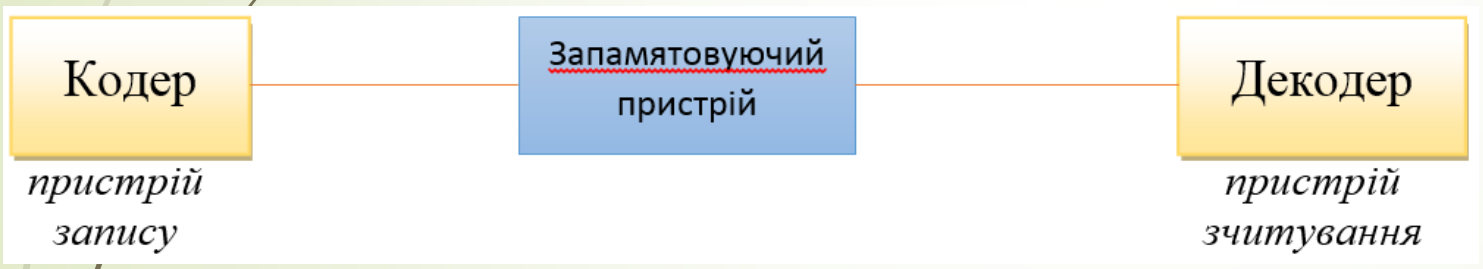


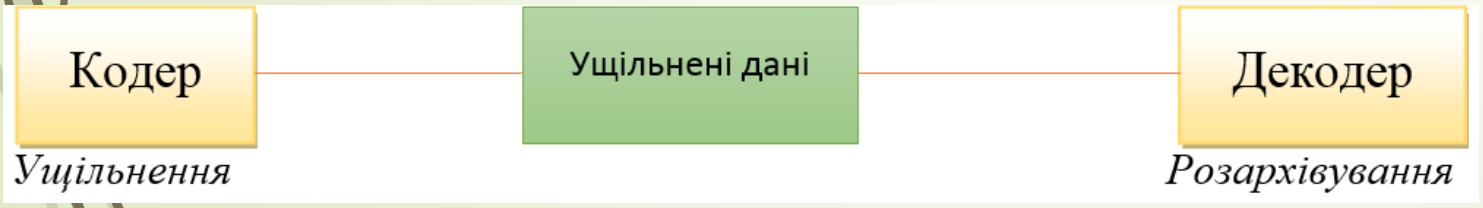
- WinRAR обчислює CRC даних і порівнює їх з CRC в архіві, і при коректності контрольної суми, розпаковує архів. Основна різниця між ним в тому, що WinRAR дозволяє відновити фізично пошкоджений файл.



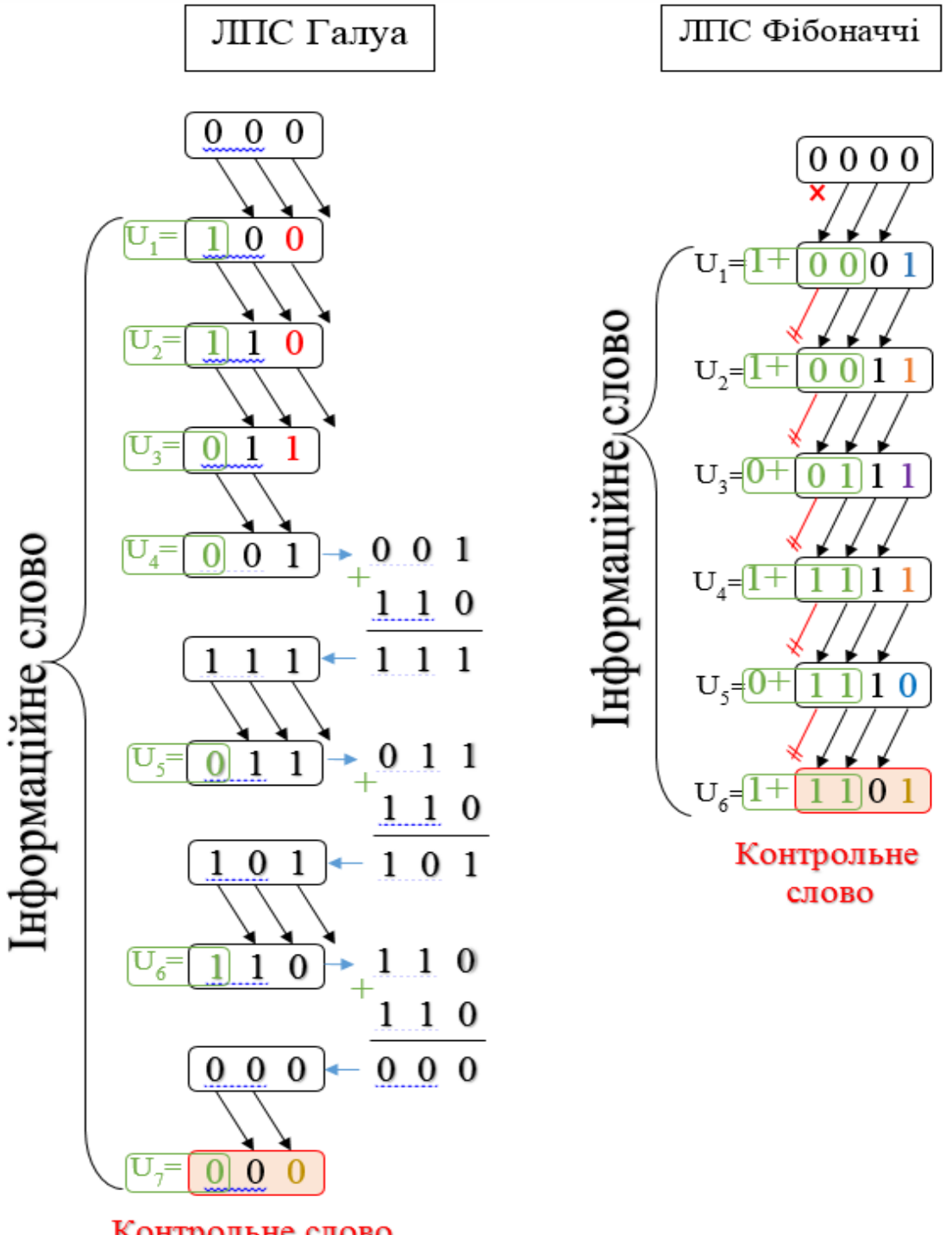
перетворення інформації







- В кожній системі передачі даних використовується своя схема перетворення інформації. Незмінними елементами в передачі даних являється наявність кодера, декодера, і каналу даних.
- **Флеш-пам'ять**
- **архівація**



Послідовне обчислення CRC за допомогою ЛПС Галуа і Фібоначчі.

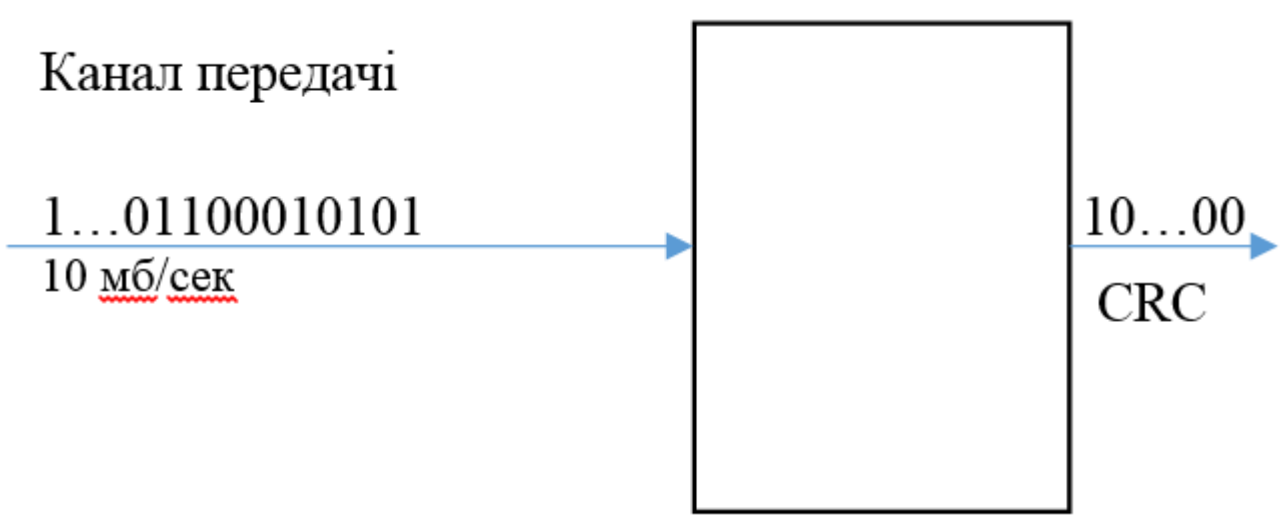
- рекурсивна ЛПС типу Галуа

$$A = \begin{vmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix}, B = \begin{vmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{vmatrix}, C = |0 \quad 0 \quad \dots \quad 1|, D = |0|$$

- рекурсивна ЛПС типу Фібоначчі

$$A = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ g_0 & g_1 & g_2 & \dots & g_{r-1} \end{vmatrix}, B = \begin{vmatrix} 0 \\ 0 \\ \dots \\ 0 \\ 1 \end{vmatrix}, C = |1 \quad 0 \quad \dots \quad 0|, D = |0|$$

Послідовний спосіб обчислення CRC




```
110011101011 | 11011   Поліном
11011
--------
00010110
   11011
--------
  011011
   11011
--------
    0011   Залишок (контрольна сума)
```

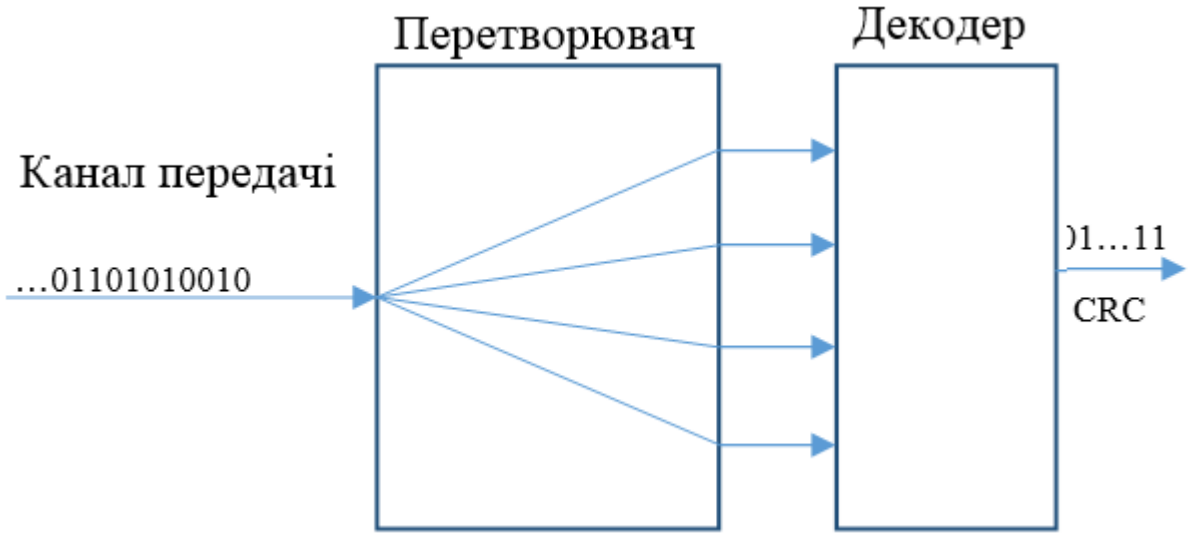
Найпростіший спосіб обчислення CRC є побітове надходження вхідних даних коли швидкість надходження даних збігається з продуктивністю їх обробки

Найбільш простий спосіб послідовного обчислення CRC - порозрядне ділення полінома

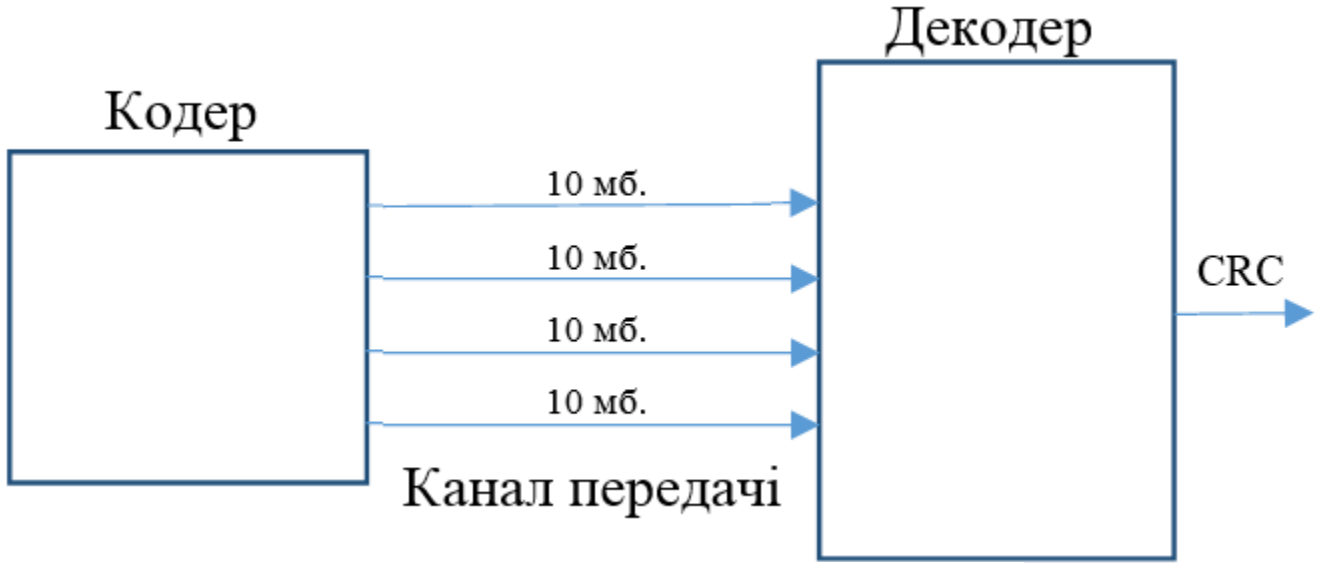
Сучасні дослідження прийшли до висновку, що найкращим розв'язанням проблеми швидкого обчислення CRC є розпаралелювання обчислень.

Засоби прискорення надходження потоків даних і підвищення продуктивності засобів обчислення CRC.

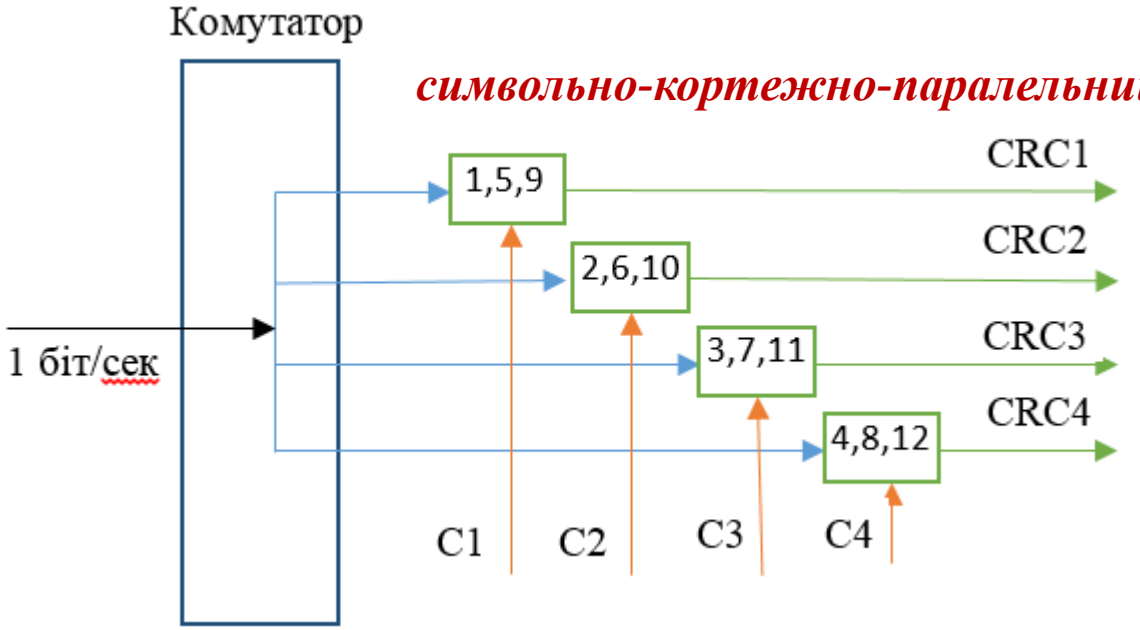
кортежно-паралельний

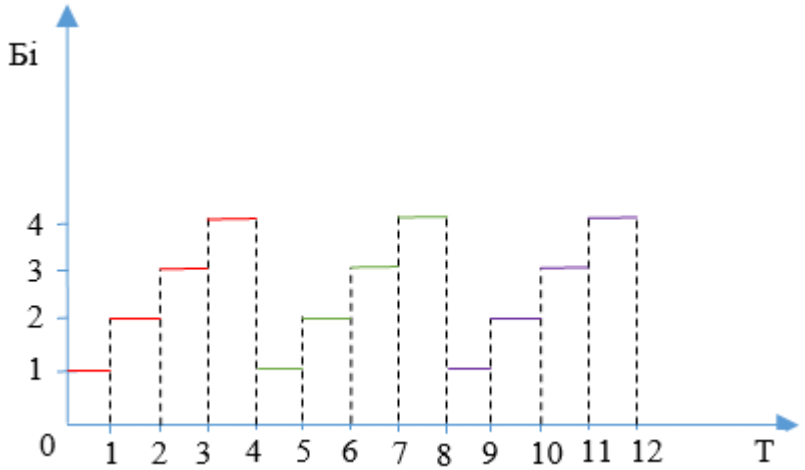


символьно-паралельний



символьно-кортежно-паралельний





Графік передачі даних кортежно-паралельного способу обчислення CRC

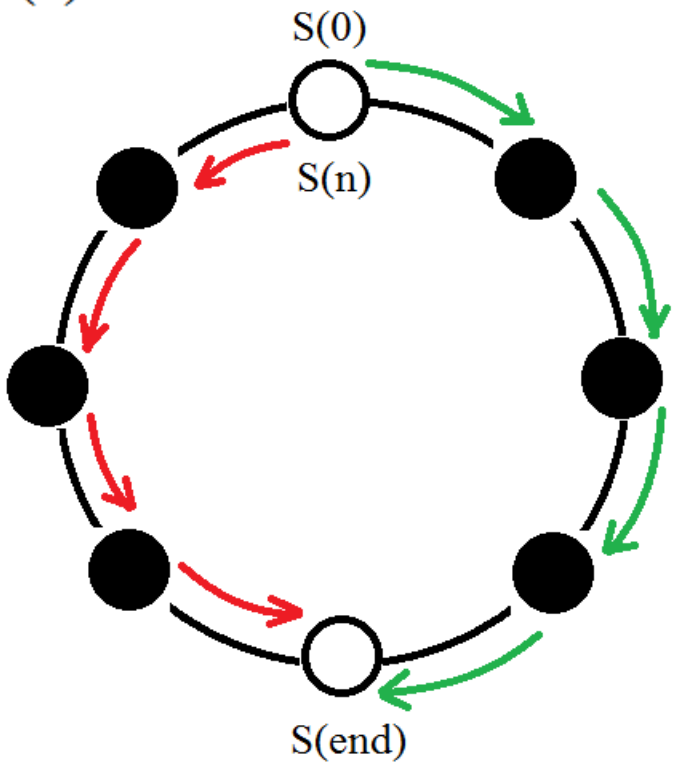
Рекурсивне CRC обчислення на основі симетрії часу

Для реверсивної ЛПС необхідно скористатись функцією переходів оберненою ЛПС з характеристичною матрицею A_{inv}:

$$S(t) = A_{inv} \times (S(t+1) + B \times U(t)), \quad GF(2).$$

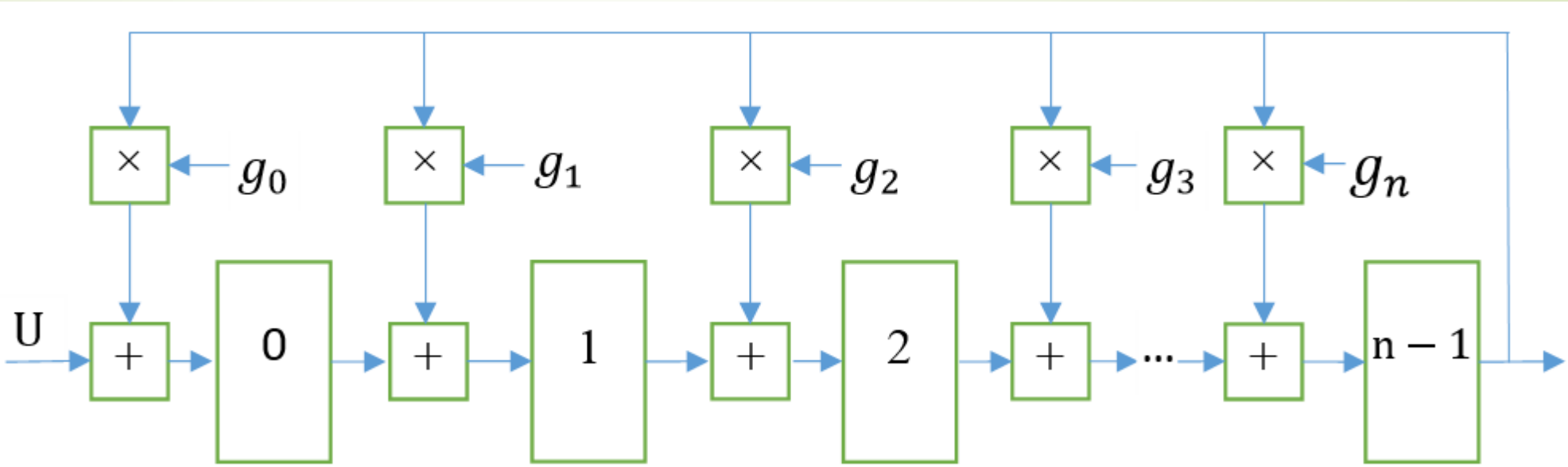
Пряма ЛПС з матрицею A визначає перехід із стану $S(t)$ в момент часу t в стан $S(t+1)$ в момент часу $(t+1)$

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2).$$



Для опису операцій декодування кодів CRC використовується ЛПС, яка реалізована у двох варіантах

Схема "Прямої" ЛПС



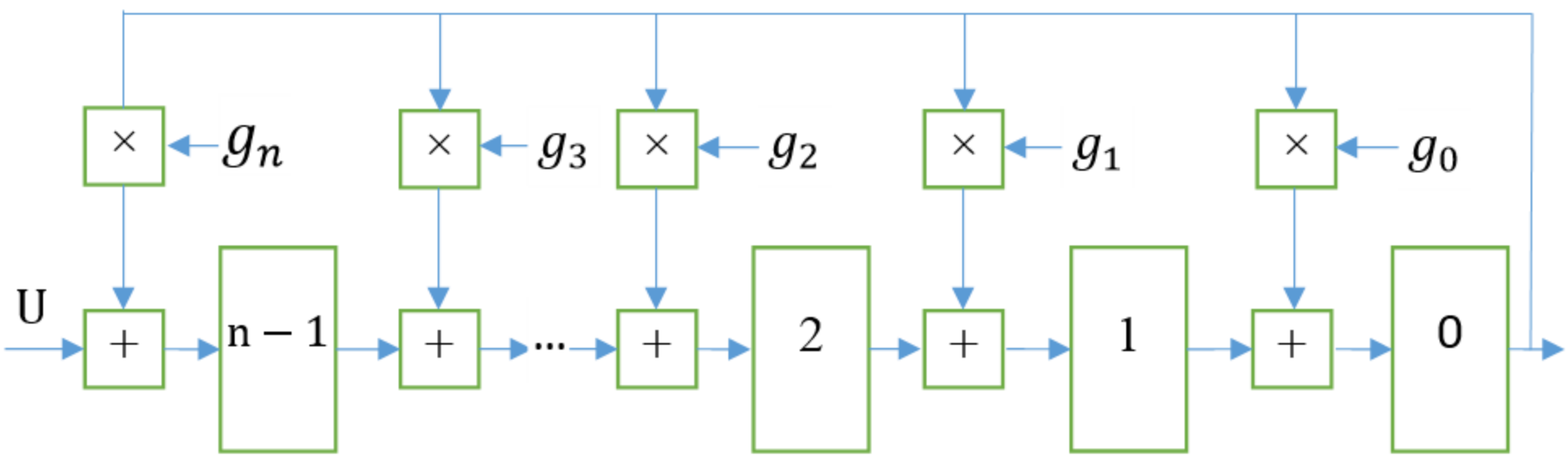
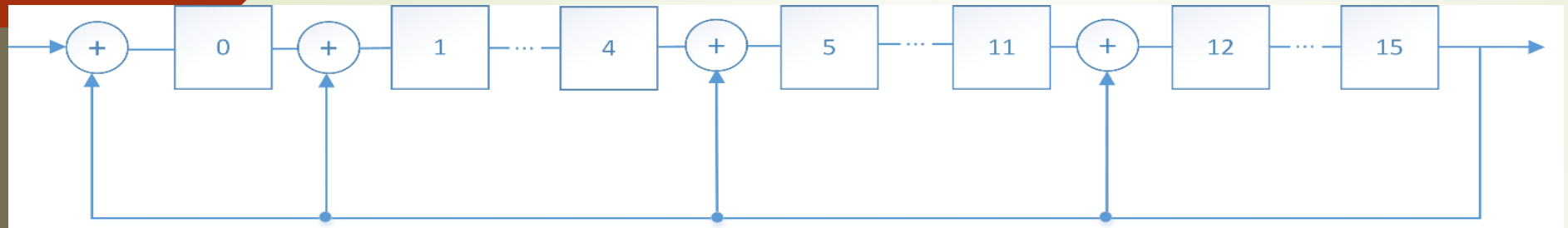


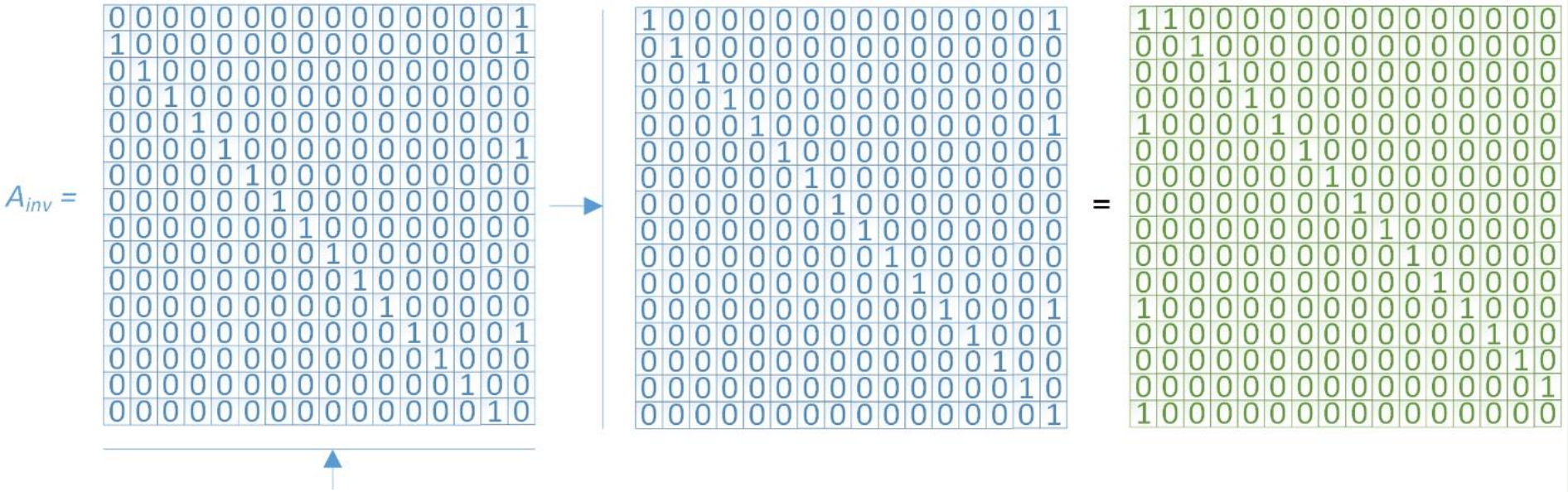
Схема "Оберненої" ЛПС

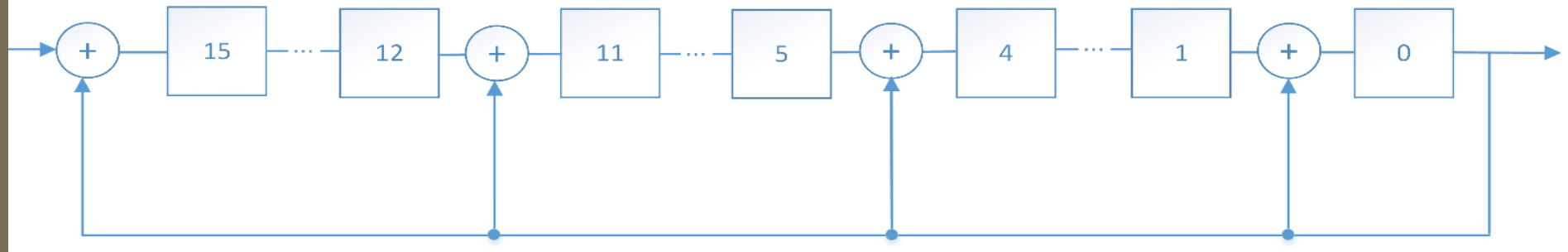
ЛПС типу Галуа для породжувального поліному:

$$g(x) = (X + 1)(X_{15} + X_{14} + X_{13} + X_{12} + X_4 + X_3 + X_2 + X + 1).$$



“Пряма” ЛПС

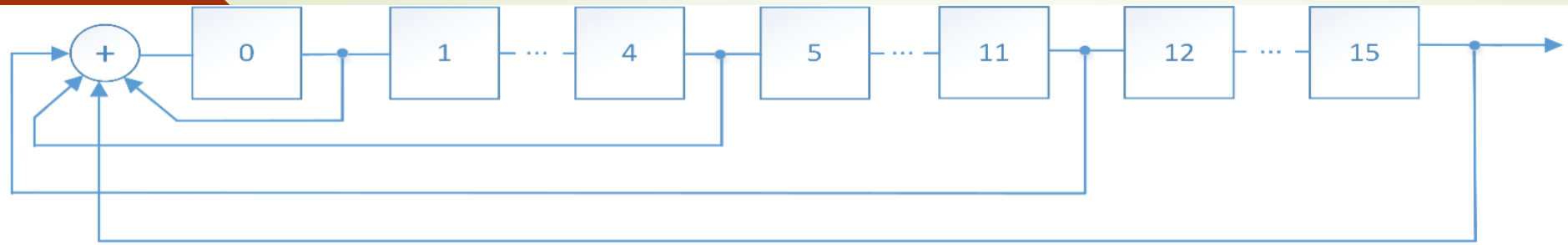




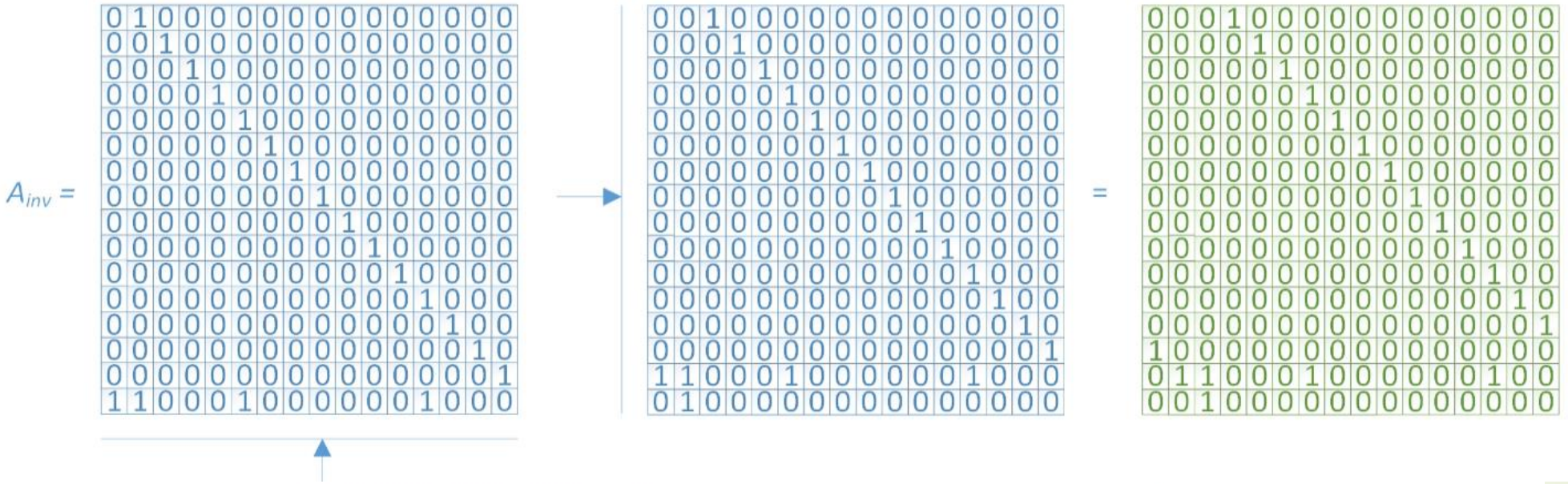
“Обернена” ЛПС

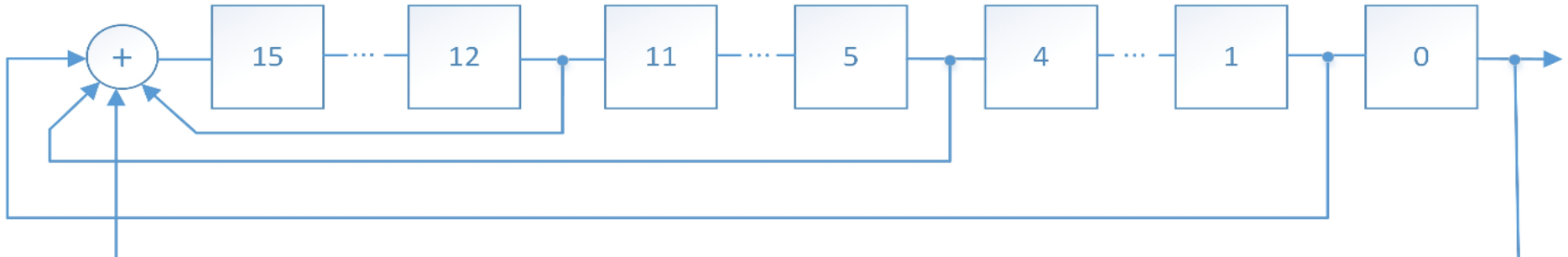
ЛПС типу Фібоначі для породжувального поліному:

$$g(x) = (X + 1)(X_{15} + X_{14} + X_{13} + X_{12} + X_4 + X_3 + X_2 + X + 1)$$



“Пряма” ЛПС





“Обернена” ЛПС

Схема паралельного обчислення CRC типу Галуа

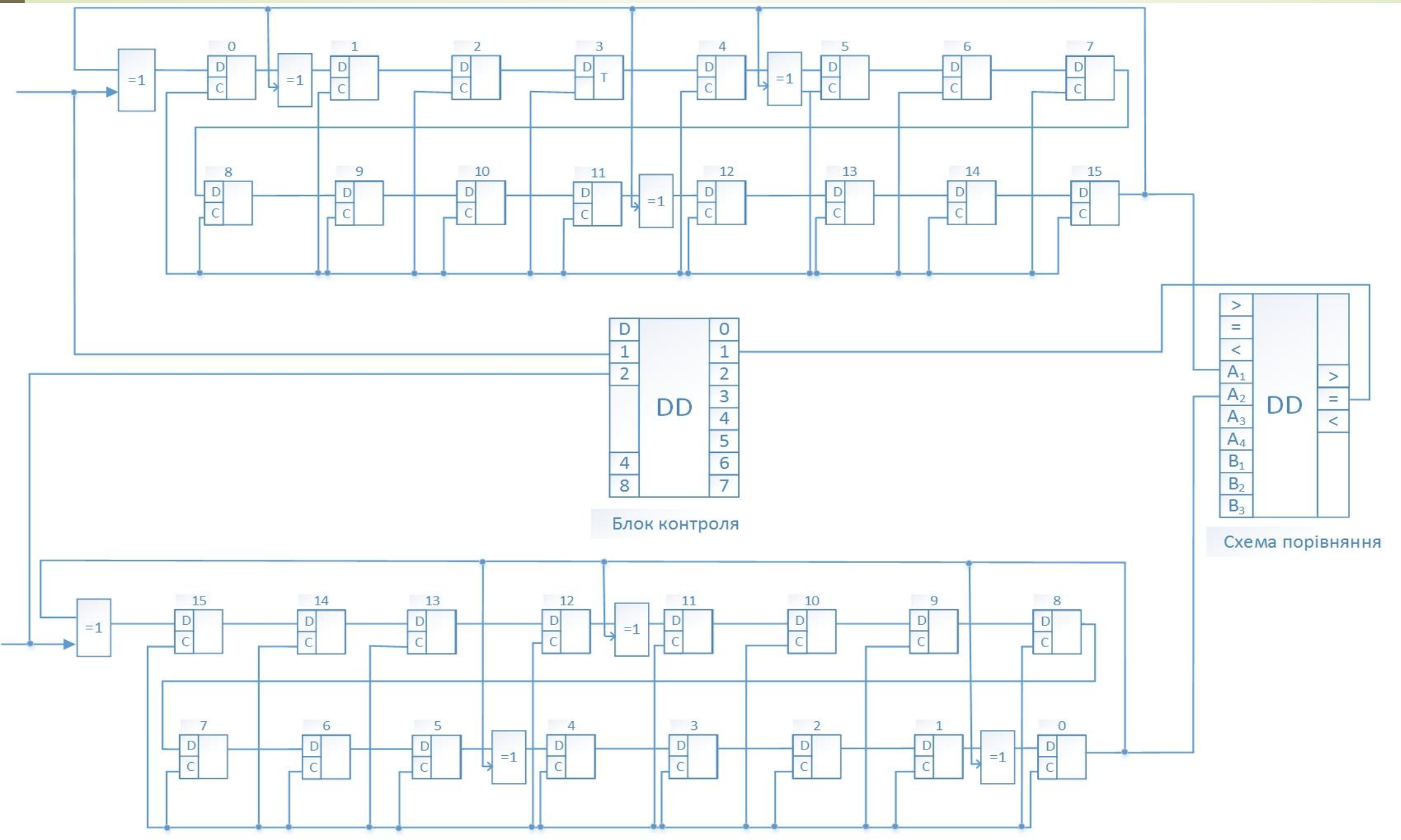
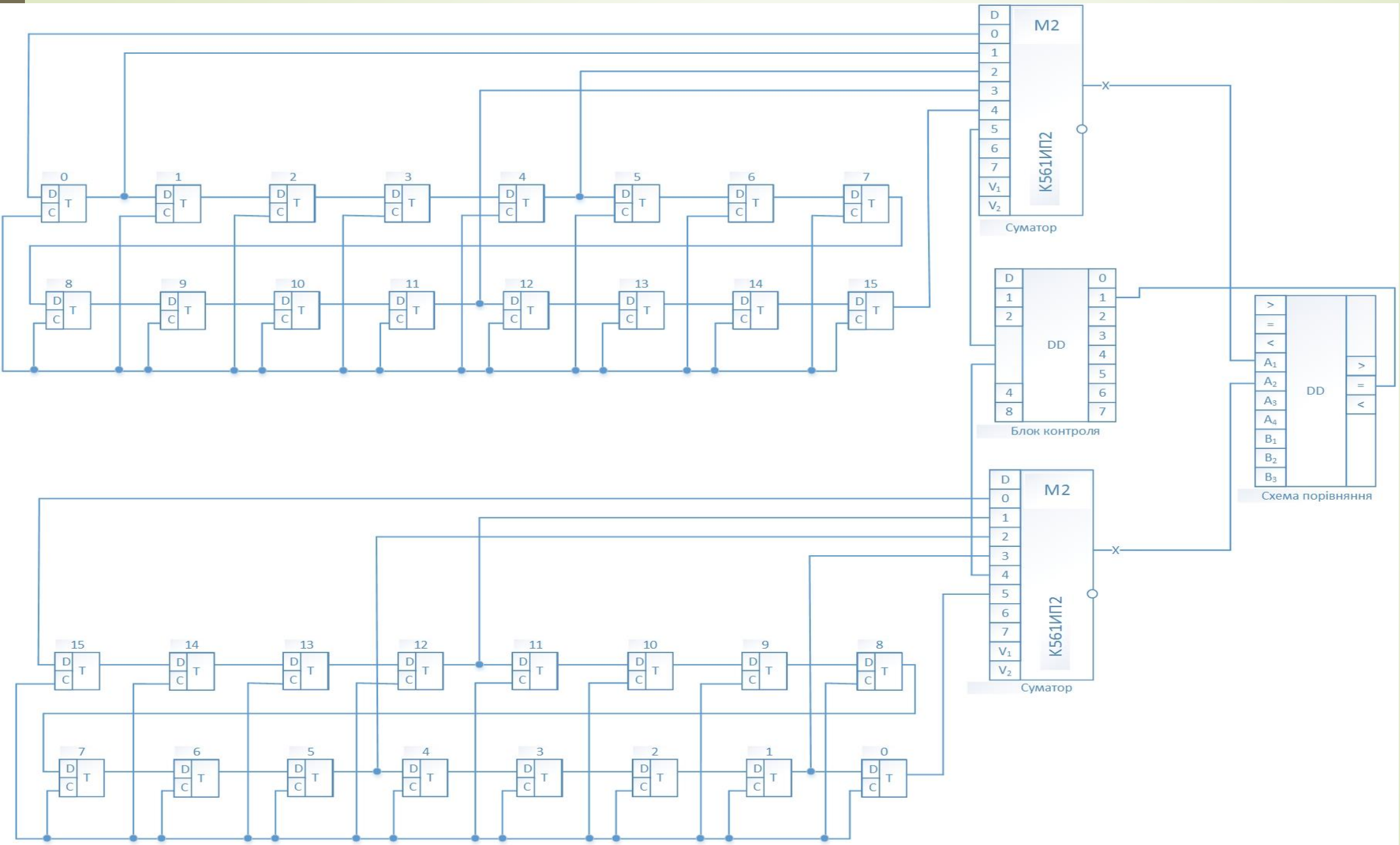


Схема паралельного обчислення CRC типу Фібоначі



Дякую за увагу