PSEUDO RANDOM GENERATOR

Budihardja Murtianta
Program Studi Teknik Elektro
Fakultas Teknik Elektronika dan Komputer– UKSW
Jalan Diponegoro 52-60, Salatiga 50711
Email: budihardja@yahoo.com

Intisari

Pada tulisan ini dirancang piranti pembangkit kode acak semu (*psendo random generator)* Piranti terdiri dari modul pengirim dan modul penerima Modul pengirim membangkitkan kode acak semu dan memodulo-2 data masukan dengan kode acak yang dibangkitkan kemudian mengirimkan data tersebut melalui kabel *coaxial* ke modul penerima. Modul penerima berfungsi menerima data dari modul pengirim, membangkitkan kode acak yang sama dengan kode acak pada modul pengirim dan memodulo-2 data yang diterima dengan kode acak tersebut. sehingga akan kembali menjadi data asli. Modul pengirim dan modul penerima merupakan modul yang sama yang berbeda hanya perangkat lunaknya. Kode acak semu yang dipakai dan dibandingkan adalah *Linier Code dan Gold Code.* Kode acak semu dibangkitkan oleh Mikrokontroler.

Kata kunci : Pseudo random generator, Modulo-2, *Linier Code, Gold Code*

1. Pendahuluan

Dengan makin banyaknya pengguna telekomunikasi, maka dibutuhkan suatu sistem komunikasi yang kebal derau, anti *jamming* dan memiliki keandalan baik. Salah satu metode yang dipakai adalah sistem spektrum tersebar yang memungkinkan banyak pemakai (*user*) dapat memakai sebuah jalur transmisi komunikasi pada waktu yang sama serta memiliki frekuensi pembawa (*carrier*) yang sama. Pemakai hanya dibedakan oleh kode tertentu yang berasal dari PRG (*Psendo Random Generator*) dan jumlah variasi kode acak semu yang dibangkitkan PRG akan membatasi jumlah

pemakai. Mengingat pentingnya peranan PRG dalam sistem spektrum tersebar maka pada tulisan ini akan dibahas suatu piranti PRG dengan menggunakan mikrokontroler MCS-51. Modul pengirim dan modul penerima merupakan modul yang sama yang berbeda hanya perangkat lunaknya. Modul pengirim terdiri dari Modul Mikrokontroler, Modul *Keyboard* IBM-PC, Modul Penampil LCD, Modul Penampil LED dan Modul Max232CPE.

2. PRG (*Pseudo Random Generator*)

PRG adalah pembangkit kode yang terdiri dari urutan yang acak (*random*) namun semu (*psendo*), karena urutan tersebut akan mengalami perulangan pada periode tertentu. Cara paling umum untuk membangkitkan kode acak adalah dengan menggunakan register geser (*shift register*). Pembangkit kode acak yang menggunakan register geser dapat digolongkan dalam 2 jenis yaitu pembangkit kode Linier (*Linier Code Generator*) dan pembangkit kode gabungan (*Composite Code Generator*). Metode pembangkitan kode Linier adalah teknik pembangkitan yang paling sederhana dan merupakan dasar metode pembangkitan yang lainnya. Metode pembangkitan kode gabungan menggunakan lebih dari sebuah pembangkit kode Linier dan variasi kode yang dihasilkan jauh lebih banyak daripada yang dapat dihasilkan oleh pembangkit kode Linier. Kode Gold merupakan kode gabungan yang sederhana pembangkitannya, dan dapat menghasilkan variasi kode yang banyak serta memiliki karakteristik korelasi tertentu. Semakin banyak register geser yang digunakan untuk membentuk PRG maka akan semakin panjang kode acak yang dihasilkan dan semakin banyak variasi kode acak yang dihasilkan. Tap atau disebut juga umpan balik berguna untuk menentukan letak umpan balik dalam suatu PRG. Letak tap berpengaruh pada panjang kode acak yang dihasilkan.

2.1. Ciri Keacakan

PRG terlihat acak karena memenuhi ciri keacakan (*randomness properties*) yaitu :

A . Ciri Keseimbangan (*Balance Property*)

Suatu kode dapat dikatakan memiliki keseimbangan yang baik bila jumlah bilangan biner '0' dan '1' dalam urutan kode tersebut hanya berselisih satu .

B . Ciri Keruntunan (*Run Property*)

Keruntunan dapat didefinisikan sebagai deretan bilangan biner yang sejenis. Panjang runtun adalah jumlah bilangan ('0' dan '1') dalam sebuah runtun. Sebuah kode dikatakan memenuhi ciri keruntunan apabila setengah dari kode tersebut memiliki panjang runtun 1 (untuk kedua jenis bilangan), seperempatnya adalah bilangan dengan panjang runtun 2, seperdelapannya adalah bilangan dengan panjang runtun 3 dan seterusnya.

Tabel 1. Distribusi Keruntunan untuk SR 5 Tingkat.

Panjang Runtun = p	Jumlah Panjang Runtun		Jumlah Chip
	' 1 '	' 0 '	
1	4	4	8
2	2	2	8
3	1	1	6
4	0	1	4
5	1	0	5
Total =	8	8	Total = 31 Chip

Rumus untuk menghitung jumlah panjang runtun adalah 2^{n-p-2} dimana n = jumlah SR dan p = panjang runtun. Ada pengecualian bahwa hanya ada satu deret biner '1' yang memiliki panjang runtun n dan hanya ada satu deret biner '0' yang memiliki panjang runtun n-1. Dari Tabel 1 terlihat bahwa jumlah panjang runtun '1' dan '0' untuk p = 1 adalah setengah dari jumlah panjang runtun total (1/2 dari 8). Jumlah panjang runtun '1' dan '0' untuk p = 2 adalah seperempat dari jumlah panjang runtun total (1/4 dari 8) dan seterusnya. Hasil dari Tabel 1 membuktikan bahwa kode yang dimaksud memenuhi ciri keruntunan.

C . Ciri Korelasi (*Correlation Property*)

Sebuah kode yang memiliki periode tertentu apabila dibandingkan dengan kode itu sendiri dengan pergeseran memutar (*cyclic shift*), dikatakan memenuhi ciri korelasi apabila jumlah chip yang sama dan jumlah chip yang berbeda hanya berselisih satu.

Contoh perhitungan nilai korelasi sebuah kode PN :

Kode I : **0** 0 0 1 0 0 1 1 0 1 0 1 1 1 1

Kode II : 1 **0** 0 0 1 0 0 1 1 0 1 0 1 1 1

b s s b b s b s b b b s s s

Kode II adalah replika kode I yang telah digeser satu chip. Bila chip yang sama ditandai dengan 's' sedangkan chip yang berbeda ditandai dengan 'b' terlihat bahwa jumlah chip yang sama dengan jumlah chip yang berbeda hanya berselisih satu dengan jumlah chip yang berbeda selalu lebih banyak satu chip dari jumlah chip yang sama.

2.2. Urutan Maksimal

Sebuah kode PN disebut sebagai kode PN urutan maksimal jika kode PN tersebut memenuhi semua syarat keacakan dan syarat – syarat tambahan berikut :

1. Syarat Panjang maksimal (*Maximal Length*)

Kode urutan maksimal harus merupakan kode yang terpanjang yang dapat dihasilkan oleh sebuah register geser (*shift register*) dengan jumlah tingkat tertentu. Sebuah register geser n tingkat dapat menghasilkan kode dengan panjang (periode) $2^n - 1$ chip .

2. Jumlah biner '1' selalu lebih banyak satu buah dibandingkan nilai biner '0'. Rumus untuk jumlah ' 1 ' adalah 2^{n-1} sedangkan rumus untuk jumlah ' 0 ' adalah $2^{n-1} - 1$. Syarat ini mempertegas ciri keseimbangan .

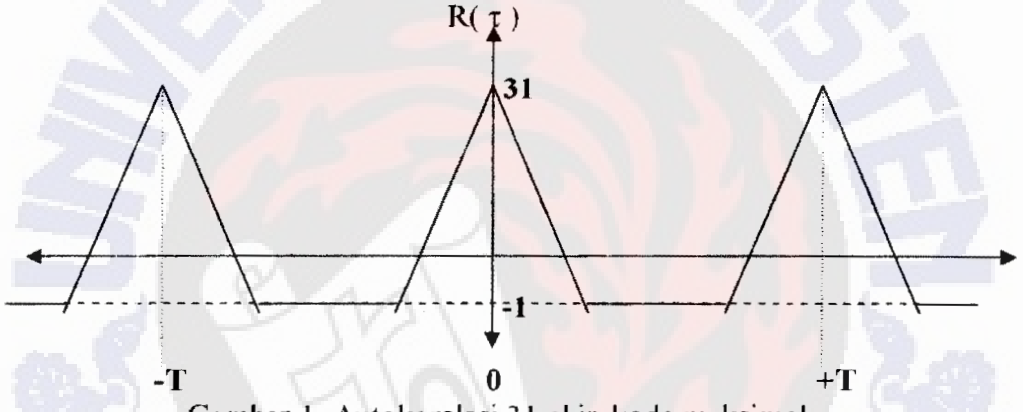
3. Syarat Statistik (*Statistical Distribution*)

Penyebaran bilangan biner ' 0 ' dan ' 1 ' selalu tetap dan tertentu . Artinya jumlah panjang runtunnya selalu dapat dipastikan . Syarat ini sama dengan ciri keruntunan. Penyebaran bilangan biner '1' dan '0' selalu tetap dan tertentu maksudnya adalah kode PN yang terdiri dari urutan kode bilangan biner '1' dan '0' dimana bilangan biner '1' dan '0' itu mempunyai aturan dalam penderetannya, aturan penderetannya adalah setengah dari jumlah panjang runtun total memiliki panjang runtun 1 (½ dari 8 untuk kedua jenis bilangan) , seperempat dari jumlah panjang runtun total memiliki panjang runtun 2 (1/4 dari 8 untuk kedua jenis bilangan) dan seterusnya. Ciri ini disebut juga *one - zero distribution* seperti yang telah dijelaskan pada ciri keruntunan. Misalkan ada kode PN sebagai berikut : 11111000110111010100001001011 00. Dari kode PN itu terlihat bilangan biner '1' yang mempunyai panjang runtun 5 ada 1, biner '1' yang mempunyai panjang runtun 4 tidak ada, biner '1' yang mempunyai panjang

runtun 3 ada 1, biner '1' yang mempunyai panjang runtun 2 ada 2, biner '1' yang mempunyai panjang runtun 1 ada 4, bilangan biner '0' yang mempunyai panjang runtun 5 tidak ada , biner '0' yang mempunyai panjang runtun 4 ada 1, biner '0' yang mempunyai panjang runtun 3 ada 1, biner '0' yang mempunyai panjang runtun 2 ada 2, biner '0' yang mempunyai panjang runtun 1 ada 4, hal ini sesuai dengan ciri keruntunan/syarat distribusi.

4. Syarat Autokorelasi

Autokrelasi kode maksimal akan selalu bernilai -1, kecuali untuk pergeseran 0 , $\pm \tau$, $\pm 2\tau$ dan seterusnya akan bernilai 2^n-1 (dengan τ adalah periode dan n adalah jumlah tingkat register geser)



Gambar 1. Autokorelasi 31 chip kode maksimal

Dari Gambar 1 terlihat bahwa nilai autokorelasi kode diatas selalu bernilai –1 kecuali pada pergeseran 0, $\pm \tau$, $\pm 2\tau$, dan seterusnya (T = 31 karena jumlah SR yang digunakan 5) sehingga memenuhi ciri autokorelasi.

5. Penambahan secara modulo

Penjumlahan secara modulo-2 suatu kode dengan replikanya , yaitu kode itu sendiri yang telah diberi tundaan tertentu akan menghasilkan replika yang lain dari kode tersebut. Sebagai contoh :

Kode asli	:	1111100011011101010000100101100
Pergeseran satu chip	:	0111110001101110101000010010110
Penjumlahan modulo-2	:	1000010010110011111000110111010

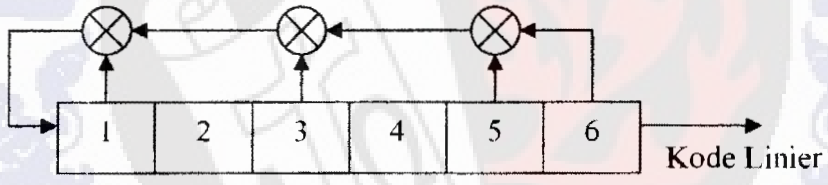
Bilangan yang dicetak tebal sebagai tanda untuk mulai membandingkan kode asli dengan kode hasil mod-2. Ternyata hasil penjumlahan modulo-2 antara kode asli

dengan replikanya yang telah digeser satu chip akan menghasilkan replika yang lain yang tergeser 14 chip dari kode asli.

6. Saat pembentukan sebuah kode dengan n-tingkat register geser semua kemungkinan kondisi biner (*n-tuple*) akan muncul pada register geser tersebut, kecuali kondisi semua nol (*all zero condition*). Semua kondisi biner hanya akan muncul sekali saja.

3. Pembangkit Kode Linier

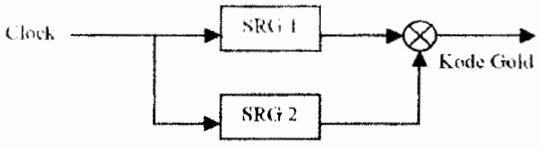
Teknik pembangkitan kode linier adalah teknik pembangkitan yang paling sederhana dan merupakan dasar teknik pembangkitan yang lainnya. Suatu pembangkit kode linier hanya dapat membangkitkan satu variasi kode acak semu. Pembangkit kode Linier dibedakan satu dengan yang lainnya dari letak tap-nya. Gambar 2 adalah gambar pembangkit kode Linier dimana tiap kotak berangka melambangkan tingkat, sedangkan bulatan melambangkan penjumlahan *EXOR*.



Gambar 2. Pembangkit Kode Linier 6 tingkat dengan letak tap [6,5,3,1] .

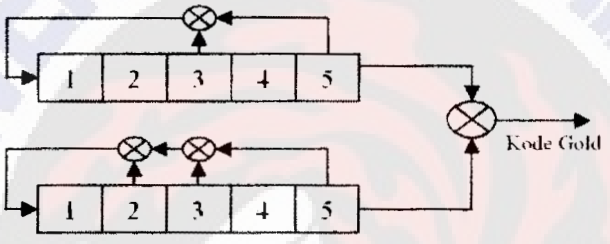
4. Pembangkit Kode Gold

Pembangkit kode Gold dapat menghasilkan variasi kode acak semu yang sangat banyak, dan hanya memerlukan sepasang pembangkit kode Linier. Keuntungan lain dari kode Gold adalah kemudahan, kesederhanaan dan kecepatan pembangkitannya. Pembangkit kode Gold yang paling sederhana (Gambar 3) hanya terdiri dari dua buah SSRG (*Simple Shift Register Generator*), masing – masing dengan satu tap. Sepasang pembangkit kode Linier dengan jumlah sama dapat digabungkan (*EXOR*) untuk membentuk pembangkit kode Gold. Kode Linier dengan panjang maksimal yang membentuk kode Gold dinamakan kode basis.



Gambar 3 Bagan kotak Pembangkit Kode Gold.

Pembangkit kode Gold 5 tingkat yang dibentuk dari penjumlahan mod-2 sepasang kode basis 5 tingkat dengan letak tap [5,3] dan [5,3,2] seperti pada Gambar 4. Panjang kode Gold yang dibangkitkan akan sama dengan panjang kode basisnya. Bila salah satu kode basis digeser maka akan terbentuk kode Gold yang lain, dengan cara ini dapat dibentuk banyak variasi kode Gold.



Gambar 4. Pembangkit kode Gold 5 tingkat dengan letak tap [5,3] dan [5,3,2].

Pembentukan kode Gold dan variasinya dengan menggunakan pembangkit seperti Gambar 4 adalah sebagai berikut :

Pergeseran 0 chip :

[5,3] : 11111000110111010100001001011 00

[5,3,4,2] : 11111001001100001011010100011 10

Kode Gold : 00000001111011011111011101000 10

Pergeseran 1 chip :

[5,3] : 11111000110111010100001001011 00

[5,3,4,2] : 11110010011000010110101000111 01

Kode Gold : 00001010101111000010100001100 01

Pergeseran 2 chip :

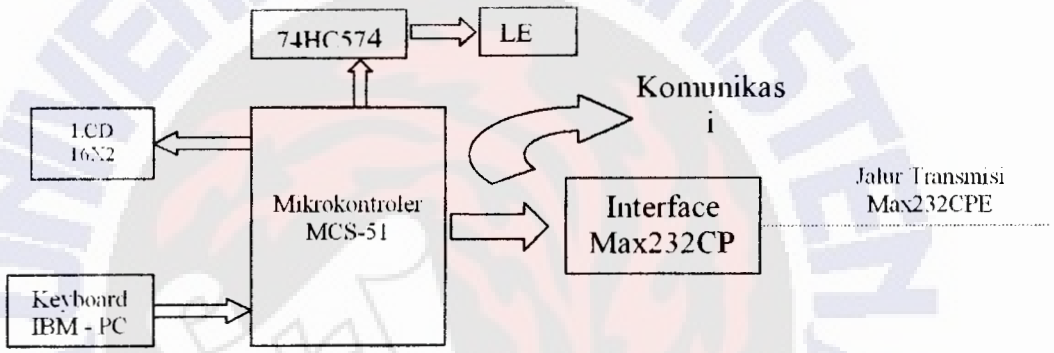
[5,3] : 11111000110111010100001001011 00

[5,3,4,2] : 11100100110000101101010001110 11

Kode Gold : 00011100000111111001011000101 11

Pada contoh tersebut, variasi kode Gold dihasilkan dengan menggeser kekiri kode basis [5,4,3,2]. Sebenarnya , arah pergeseran dan kode basis mana yang digeser tidak akan mempengaruhi jumlah variasi kode Gold yang dihasilkan. Semua kode Gold yang dihasilkan pada contoh diatas tidak ada yang sama. Karena panjang kode basis 31 chip ($2^5 - 1$), maka τ (pergeseran) maksimum yang dapat dilakukan adalah 30 chip ($\tau = 31$ sama dengan $\tau = 0$) Jadi dengan sepasang pembangkit kode basis 5 tingkat, dapat dibentuk 31 varian kode Gold.

5. Piranti PRG



Gambar 5. Blok Diagram Modul Pengirim

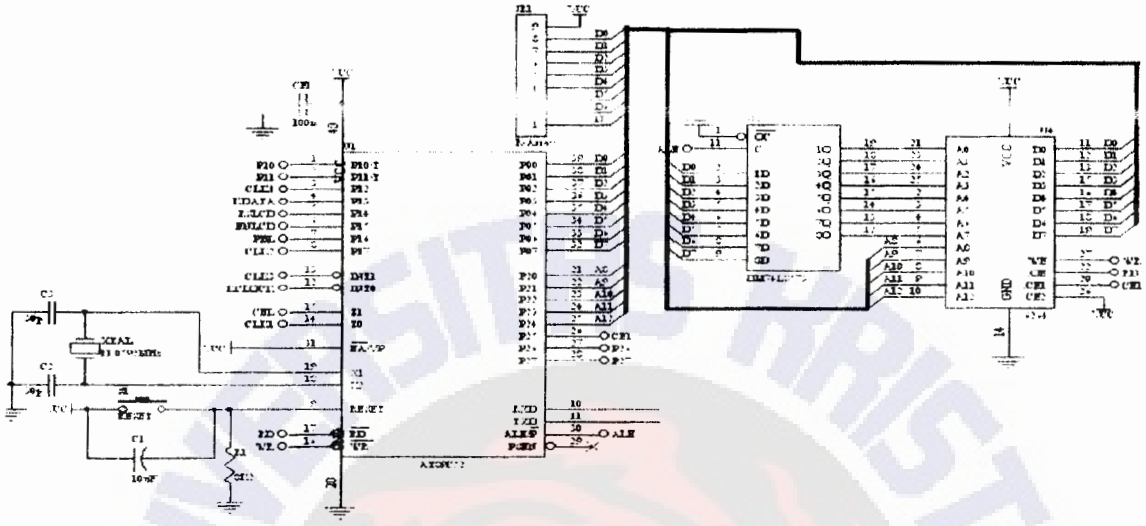
Gambar 5 menunjukkan Modul Pengirim yang terdiri dari :

1. Modul Mikrokontroler
2. Modul Penampil LCD
3. Modul Keyboard IBM – PC
4. Modul Penampil LED
5. Modul Max232CPE

5.1. Modul Mikrokontroler

Modul mikrokontroler sebagai modul utama sistem (Gambar 6), disusun dengan mikrokontroler AT89C52 produksi *Atmel semiconductors* dengan osilator kristal 11.0592 (MHz) dilengkapi dengan *IC latch* (74HC573), dan *IC SRAM* (6264). Adapun alasan memilih AT89C52 karena memiliki internal EPROM sebesar 8 K dan mudah diprogram. Modul ini berfungsi menghasilkan kode acak, mengambil data input dari *keyboard* standar IBM, menampilkan menu pilihan dan kondisi yang dipilih (metode, jumlah

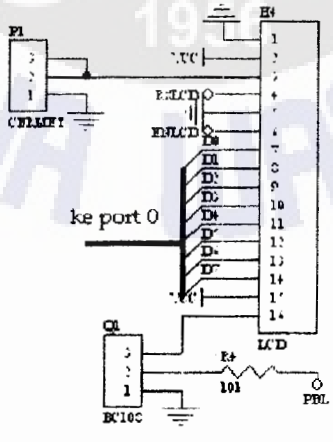
register geser, letak tap, nilai awal dan data yang akan dikirim) ke Penampil LCD, menampilkan pilihan kondisi (jumlah register geser, letak tap, nilai awal dan kode acak yang dihasilkan) ke Penampil LED dan menyimpan Kode acak yang dihasilkan di RAM.



Gambar 6. Modul Mikrokontroler

5.2. Modul Penampil LCD

Penampil menu pilihan menggunakan LCD (*Liquid Crystal Display*) karena tampilan fisik dan kemampuan menampilkan huruf jauh lebih baik dari pada *seven segment*. LCD yang digunakan adalah LCD 16x2 karakter dilengkapi lampu *background* (*backlight*). Modul Penampil LCD seperti Gambar 7.



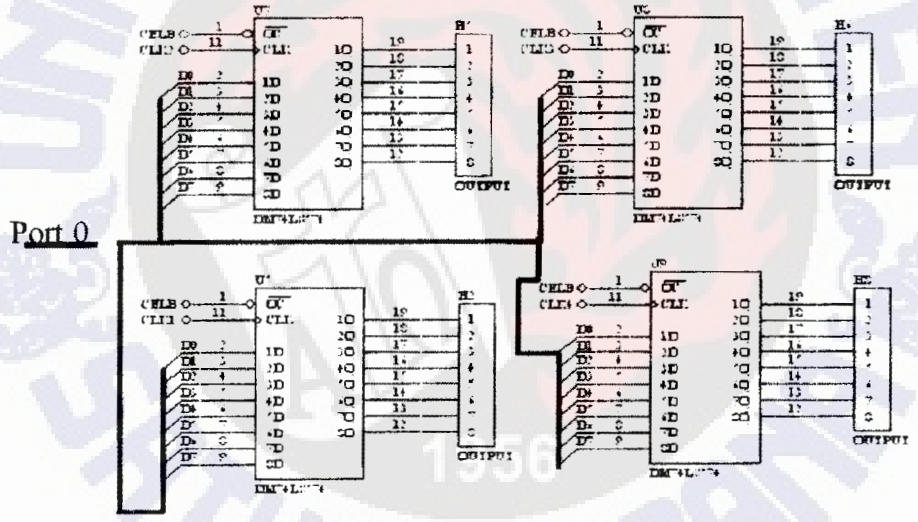
Gambar 7. Modul Penampil LCD.

5.3. Modul *Keyboard* IBM - PC

Modul *Keyboard* IBM-PC digunakan untuk mengeset metode pembangkitan kode acak, jumlah register geser, letak tap, nilai awal dan data masukkan yang diinginkan. *Keyboard* standar IBM sering disebut *keyboard* 101 tombol. *Keyboard* ini dipilih karena familiar dangan pengguna.

5.4. Modul Penampil LED

Modul penampil LED terdiri dari 3x8 LED dan 1x16 LED, sebuah resistor 220 ohm dan 4 IC 74HC574 seperti terlihat pada Gambar 3.9. Modul ini digunakan untuk menampilkan jumlah register geser, letak tap dan nilai awal yang diinginkan , juga untuk menampilkan proses pembangkitan kode PN. Diagram alir Inisialisasi IC *Latch* 74HC574 seperti pada Gambar 8.

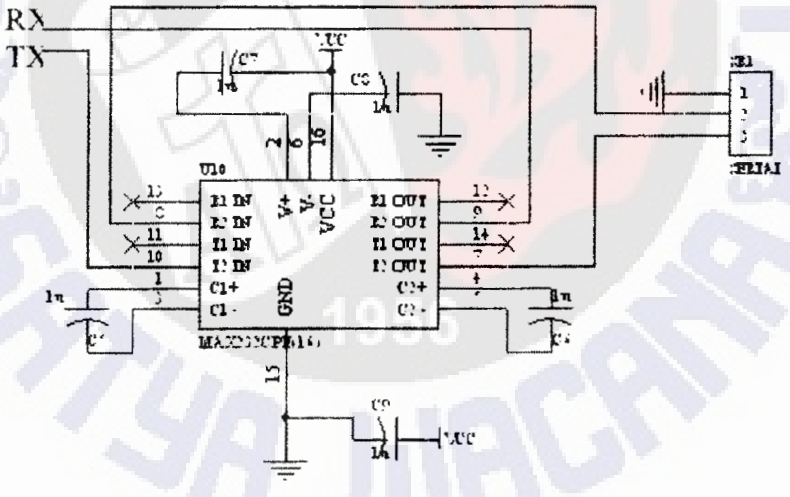


Gambar 8. Modul Penampil LED.

5.5. Modul Max 232CPE

Untuk komunikasi serial Max 232 digunakan *IC* Max232CPE buatan Texas Instrument. Hubungan antara Max 232CPE dan mikrokontroler AT89C52 dapat dilakukan secara langsung karena keduanya bekerja pada level TTL. Komunikasi data menggunakan komunikasi data serial secara asinkron. Mode Operasi Port Serial yang digunakan adalah Mode 1 UART 8 Bit dengan *Boud Rate* yang dapat diatur . Pada mode ini komunikasi data dilakukan secara 8 bit data asinkron yang terdiri dari 10 bit, yaitu 1 bit start, 8 bit data dan 1 bir stop. Boud Rate pada mode ini dapat diatur dengan

menggunakan Timer 1. Pada mode ini yang merupakan mode UART, fungsi-fungsi alternatif dari P3.0/RXD dan P3.1/TXD digunakan. P3.0 yang berfungsi sebagai RXD yaitu kaki untuk penerimaan data serial dihubungkan dengan pin 9 Max232CPE dan P3.1 yang berfungsi sebagai TXD yaitu kaki untuk pengiriman data serial dihubungkan dengan pin 10 Max232CPE. Pengiriman data dilakukan dengan menuliskan data yang akan dikirim ke Register SBUF. Data serial akan digeser keluar diawali dengan bit start dan diakhiri dengan bit stop dimulai dari bit yang berbobot terendah (LSB) hingga bit berbobot tertinggi (MSB). Bit TI akan set setelah bit stop keluar melalui kaki TXD yang menandakan proses pengiriman data telah selesai. Bit ini harus di-*clear* oleh perangkat lunak setelah pengiriman data selesai. Penerimaan data dilakukan oleh mikrokontroler dengan mendeteksi adanya perubahan kondisi dari logika high ke logika low pada kaki RXD. Perubahan kondisi tersebut merupakan bit start. Selanjutnya data serial akan digeser masuk ke dalam SBUF dan bit stop ke dalam bit RB8. Bit RI akan set setelah 1 byte data diterima ke dalam SBUF kecuali jika bit stop = 0 pada komunikasi multiprosesor (SM2 = 1). Modul Max 232CPE dapat dilihat pada Gambar 9 berikut ini.



Gambar 9. Modul Max 232CPE.

6. Hasil Pengujian

Tabel 2. Kode PN hasil Pengujian dengan kode PN hasil Perhitugan menurut teori.

Metode	Jumlah Register	Letak tap	Nilai Awal	Kode PN Hasil Pengujian	Kode PN Hasil Perhitungan
Linier	2	[2,1]	11	110	110
Linier	2	[2,1]	01	101	101
Linier	2	[2,1]	10	011	011
Linier	3	[3,1]	111	1110100	1110100
Linier	3	[3,1]	110	0111010	0111010
Linier	3	[3,1]	101	1010011	1010011
Linier	3	[3,1]	100	0011101	0011101
Linier	4	[4,1]	1111	111101011001000	111101011001000
Linier	4	[4,1]	1110	011110101100100	011110101100100
Linier	4	[4,1]	1101	101100100011110	101100100011110
Linier	5	[5,2]	11111	1111100110100100 0010101110110000	1111100110100100 0010101110110000
Gold	5	[5,2]	11111	0000000010010100	0000000010010100
	5	[5,4,3,2]	11111	0011110101011000	0011110101011000

Dari Tabel 2 terlihat kode acak hasil Pengujian sama dengan kode acak hasil perhitungan secara teori sehingga dapat disimpulkan bahwa piranti PRG sudah bekerja dengan baik dapat membangkitkan kode acak sesuai dengan teori.

Pengujian komunikasi serial antar modul dilakukan dengan mengirimkan data sederhana (data masukkan yang sudah dimodulo-2 dengan kode PN). Dari pengujian yang dilakukan didapatkan hasil yaitu : data yang dikirim oleh modul pengirim dapat diterima dengan baik oleh modul penerima dan dapat di*despreading* dengan baik sehingga data yang diterima kembali menjadi data asli tanpa adanya kesalahan.

7. Kesimpulan

- PRG dapat direalisasikan pada sebuah mikrokontroler.
- Kode acak yang dihasilkan baik dengan metode Linier dan Gold sesuai dengan hasil perhitungan secara teori.
- Metode pembangkitan kode gabungan menggunakan lebih dari sebuah pembangkit kode Linier seperti halnya kode Gold menghasilkan variasi kode yang lebih banyak daripada yang dapat dihasilkan oleh pembangkit kode Linier.
- Data yang dikirimkan ke modul penerima setelah melalui proses *despreding* dapat kembali menjadi data aslinya dan hasil despeding ini ditampilkan oleh LCD modul penerima dengan baik

Daftar Pustaka

1. R .C Dixon , `` *Spread Spectrum Systems* `` , John Wiley & Sons Inc, NewYork ,1996 .
2. Rodger E . Zimer , Roger L . Peterson , `` *Digital Communication and Spead Spectrum System* `` , 1985 .
3. Charles E . Cook , Fred W . Ellersick , Laurence B . Milstein , Donald L . Schilling , `` *Spead - Spectrum Communications* `` , IEE PRESS 1983 .
4. William C . Y . Lee , `` *Mobile Cellular Telecommunications System* `` , Mc Graw – Hill Book Company .
5. Jhong Sam Lee , Leonard E . Miller , `` *CDMA System Engineering* `` , Arthech House Publishers, 1998 .
6. Savo Glisic , Branka Vucetic , `` *Spead Spectrum CDMA System for Wireless Communications* `` , Arthech House Publishers, 1998 .