

Cellular Networks

GSM, UMTS and related stuff

(C) Herbert Haas 2005/03/11



History

(C) Herbert Haas 2005/03/11

2

History (1) – Early Developments



- **1920s**
 - ◆ US police departments use (experimental) radiotelephony
 - ◆ Only maritime applications – problems with obstacles (buildings in cities)
- **1930s**
 - ◆ FM developed – better battlefield communications during 2nd WW

History (2) – “First Generation”



- **1978-1983**
 - ◆ Advanced Mobile Phone Service (**AMPS**) in Chicago
 - ◆ FDMA @ 800 MHz, 30 kHz per channel
 - ◆ AT&T-split delayed a widespread commercial system
- **1979**
 - ◆ Japan deployed AMPS
- **1981**
 - ◆ Nordic Mobile Telephony (NMT)
 - ◆ Sweden, Norway, Denmark, Finland
 - ◆ First 450 MHz, later 900 MHz (NMT900)
- **1985**
 - ◆ Total Access Communication System (TACS, just a modified AMPS)
 - ◆ 900 MHz

AMPS, NMT, and TACS are still in service today

History (3) – “Second Generation”



- **1990: IS-54B**
 - ♦ **Interim Standard (IS)** to make AMPS digitally (aka D-AMPS)
 - ♦ Digital voice channels (using TDM)
 - Allowed three simultaneous conversations on same RF channel
 - ♦ Signaling channels still analog
 - ♦ 800 MHz
- **1994: IS-136**
 - ♦ Also digital signaling channel
 - ♦ 800 and 1900 MHz (USA, “Personal Communications Service”, **PCS**)

History (4) – GSM



- **1982: Common Europe standard needed**
 - ♦ NMT not sufficient, demand for digital system
 - ♦ CEPT established GSM group (“Group Spéciale Mobile”)
- **1987: GSM Association**
 - ♦ Industry association, more than 750 members today
- **1989: ETSI founded**
- **1991: First GSM network launched**
- **1992: International roaming between various GSM networks**
- **Great success – even deployments in Australia**
 - ♦ GSM is now interpreted as “Global System for Mobile communications”
- **TDMA @ 900 MHz, later 1800 MHz (“GSM1800”)**
 - ♦ Also introduced in North America as option for PCS (1900 MHz)

History (5) – IS-95 CDMA



- **Increase the capacity: CDMA**
 - ♦ **Code Division Multiple Access: Each user is modulated with a unique code sequence**
 - Code bit rate must be much higher than information bit rate
 - ♦ **First commercial demonstration by Qualcomm in 1989, San Diego Calif.**
- **Standardized as IS-95 in 1993 by TIA**
 - ♦ **Deployment in North America and Korea**
 - ♦ **800 MHz and 1900 MHz (“J-STD-008”)**
 - ♦ **Spread Spectrum with 1.228 MChips/s**

History (6) – “Third Generation”



- **ITU released “International Mobile Telecommunications” 2000 (IMT-2000) recommendations**
 - ♦ **144 Kbit/s for mobile services and up to 2 Mbit/s for fixed services**
 - ♦ **Multimedia services**
 - ♦ **Networks with small and large number of subscribers**
 - ♦ **2 GHz**
- **ITU accepted six air interface proposals:**
 - ♦ **Wideband CDMA (WCDMA)**
 - ♦ **CDMA 2000 (evolution of IS-95 CDMA)**
 - ♦ **TD-SCDMA (time division-synchronous CDMA)**
 - ♦ **UWC-136 (evolution of IS-136)**
 - ♦ **DECT**
 - ♦ **UMTS**



Technologies

Overview



- **1G**
 - ♦ Fully analog
 - ♦ Most important standards:
 - AMPS, NMT, TACS
- **2G**
 - ♦ Digital
 - Increased capacity, security
 - Advanced services
 - ♦ Most important standards:
 - IS-136 (TDMA)
 - IS-95 CDMA (by Qualcomm)
 - Global System for Mobile communications (GSM)
- **3G**
 - ♦ Need to support data services (WWW, e-commerce, E-Mail, ...)
 - ♦ CDMA 2000, UMTS

Das "Handy" = Mobile Station (MS)

- **MS consists of**
 - ♦ Mobile Equipment (ME)
 - ♦ Subscriber Identity Module (SIM)
- **Power controlled by BS**
 - ♦ In 2dBm steps
- **Maximum power (EIRP)**
 - ♦ 2/2.5G: 4 W (3G: 2 W)

The SIM Card

- **Processor and nonvolatile memory**
- **PIN protected**
- **EAP-SIM Authentication**
- **Also used for encryption of voice and signalling data**
- **Optionally used as NVRAM for contacts, SMS, notebook, last called number list, ...**
- **SIM-Access-Profile**
 - ♦ Car connects to SIM via Bluetooth, reads authentication information and establishes GSM/UMTS connection by itself via external antenna

SMS, MMS etc



- **Short Message Service (SMS)**
 - ◆ Typically up to 160 characters
- **Enhanced Message Service (EMS)**
 - ◆ Additional formatting options (bold, italic, ...) and "emoticons"
 - ◆ No length restriction
 - But each additional 160 chars are billed as additional SMS
- **Multimedia Message Service (MMS)**
 - ◆ Consists of arbitrary attachments
 - MIME-coded text, images, or videos
 - ◆ No size restrictions specified
 - Most vendors allow only up to 50-100 kByte
 - ◆ Requires GPRS as transport layer and WAP, SOAP, SMTP on layer 7
- **Synchronized Multimedia Integration Language (SMIL)**
 - ◆ XML-based, W3C standard for slideshows
 - ◆ Extension ".smi" or ".smil"
 - ◆ SMIL2 can be embedded via XHTML or SVG

Packet Switching Issues



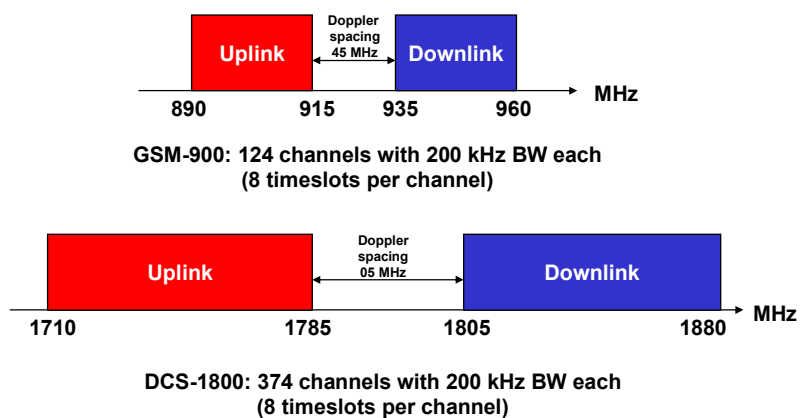
- **Volume-based billing**
- **Good handling of bursty data**
 - ◆ Statistical TDM in the backbone
- **Circuit Switched Data (CSD)**

GSM



- **Combination of FDMA and TDMA**
 - ♦ Each frequency channel carries TDMA frames with *eight* time-slots
 - ♦ Each time-slot is reserved for a single connection ("voice call")
- **Gaussian Minimum Shift Keying (GMSK) as basic modulation method**
- **Uses LAPDm for signalling**
 - ♦ A LAPD variant for mobile
- **GSM Association**
 - ♦ <http://www.gsmworld.com/>

GSM Frequencies



Mobile Station always uses lower frequencies because of lower FSL (MS has less power than BS)

GSM Technical Details (1)



- **Mobile station sends**
 - ♦ 156.25 bit every 570 usec = 270.833 kbit/s
 - ♦ 156.25 bit exactly fits in one TDMA frame
 - ♦ GMSK maps this stream to a 200 kHz channel
 - ♦ Only 22,8kbit/s usable for voice/data
- **Voice coding utilizes a combination of**
 - ♦ Linear Predictor Coding (LPC)
 - ♦ Long Term Prediction (LTP)
 - ♦ Regular Pulse Excitation (RPE)
- **RPE/LTP-LPC converts 64 kbit/s PCM into 13 kbit/s**
 - ♦ 64 kbit/s stream is segmented into 20 ms blocks (1280 bits) and subsequently encoded (LPC->LTP->RPE)
 - ♦ Additional CRC bits

GSM Technical Details (2)



- **Optional "Half-Rate Channel Technique"**
 - ♦ Utilizes as stronger encoder (CELP)
 - ♦ Results in 5.6 kbit/s streams (allows 2 users per channel)
 - ♦ Requires up to 4x battery power
 - ♦ Typically used during mass events (e. g. Donauinsselfest)
- **Optional Frequency Hopping**
 - ♦ BSS could allow mobile station to utilize e.g. four unused channels for FH

Railways: GSM-R



- European Integrated Railway radio Enhanced Network (EIRENE) Project
- Additional features
 - ♦ Train safety signalling
 - ♦ Hunt groups
 - ♦ Priority calling
- New bands
 - ♦ Uplink: 876-915 MHz
 - ♦ Downlink: 921-960 MHz (Downlink)
 - Contains GSM-900

Cells

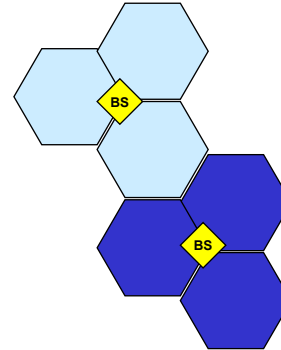


- GSM network is also called Radio Access Network (RAN)
- Any mobile radio network is “cellular”
 - ♦ Geographical coverage areas
- Each cell:
 - ♦ Has a central “**base station**” (**BS**) to connect mobile devices with the backbone network
 - ♦ Can use 1-16 frequencies
- Cell sizes vary significantly !!!
 - ♦ Depend on antennas and antenna height, obstacles, TX power
 - ♦ From 30 m to 35 km
- TX power !!!
 - ♦ 2.5 to 320 W (!)
 - ♦ Typically 10 W

Base (Transceiver) Station - B(T)S



- Use sectorized cells
 - ◆ Co-located BS for several cells
 - ◆ Directional antennas (instead of omni-)
 - ◆ Typically three 120° sectors (up to six)
 - ◆ Full duplex communication
- Main tasks
 - ◆ (De)activate assigned radio channels
 - ◆ Encryption and decryption
 - ◆ Connection control
 - ◆ Power level adaptation (TPC)
 - ◆ Signal quality measurement
 - ◆ Continuously send at constant power on all unused channels (=timeslots) to indicate BS existence to mobile nodes

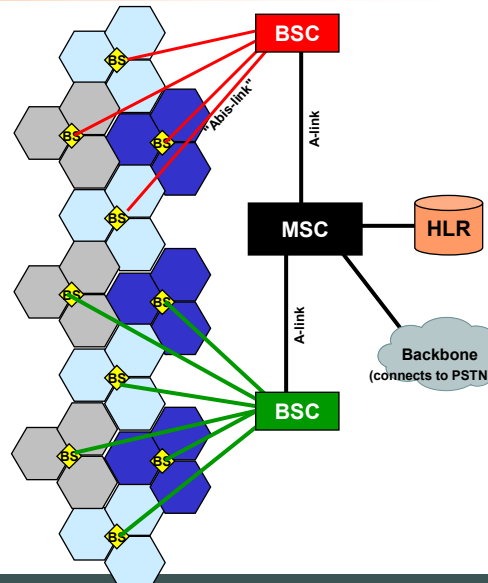


BS is also called Base Transceiver Station (BTS)

BSS and MSC



- Several Base Stations are connected to a Base Station Controller (BSC)
 - ◆ "Abis-link", typically 2 Mbit PCM
 - ◆ Manages e.g. handoff between BS
 - ◆ Receives power level and signal quality measurements from BS to support handover decisions
- Base Station Subsystem (BSS) = BSC + several BS
- Several BSS are connected to a Mobile Switching Center (MSC)
 - ◆ Via an "A-link"
 - ◆ Manages setup and teardown of CSD (voice)
 - ◆ Similar as PSTN switch
 - ◆ Aka "Mobile Telephone Switching Office (MTSO)"
- Home Location Register (HLR) contains
 - ◆ Subscription information
 - ◆ Tracks location of users: MSC notifies HLR when new users appear
 - ◆ Using the MAP Protocol (SS7)
 - ◆ Typically contains Authentication Center (AUC)



HLR Data



- **IMSI – International Mobile Subscriber Identity**
 - ♦ **MCC – Mobile Country Code**
 - 232 = Austria
 - ♦ **MNC – Mobile Network Code**
 - 01 = Mobilkom Austria
 - ♦ **HLR – Number**
 - ♦ **SN – Subscriber Number**
- **MSISDN – Mobile Subscriber ISDN Number**
 - ♦ = telephone number of subscriber
 - ♦ E. g. 43 664 20 12345
 - 43 = country code (Austria)
 - 664 = National Destination Code (NDC)
 - 20 = HLR number
 - 12345 = individual number
- **MSRN – Mobile Station Roaming Number**
 - ♦ Assigned by VLR to Mobile Station (MS)
 - ♦ Only valid as long MS remains in the area of the VLR
 - ♦ Used by HLR to localize MS (to identify remote MSC)
– allows international localization !!!
 - ♦ Consists of
 - VCC - Visitor Country Code
 - VNDC - Visitor National Destination Code ("Ortskennzahl")
 - SN - Subscriber Number = VMSC + VSN
 - VMSC - Visitor Mobile Switching Center
 - VSN - Visitor Subscriber Number

VLR - Visitor Location Register

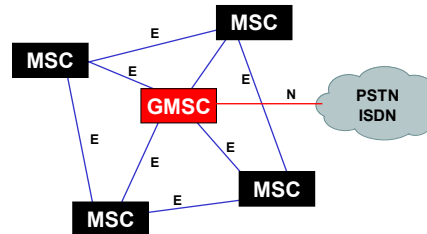


- **VLR stores temporary data of MS**
 - ♦ Removed if MS is turned off for several days
- **Each MSC is connected to a VLR**
- **VLR data contains**
 - ♦ IMSI, MSISDN, MSRN
 - ♦ TMSI – Temporary Mobile Subscriber Identity
 - ♦ LAI – Location Area Identity
 - ♦ AUC data
 - ♦ Supported services of MS
 - ♦ State of the MS

GMSC - Gateway MSC



- Is only a dedicated MSC which connects to foreign ISDN or GSM or PSTN networks
 - ♦ Gateway between own and partner networks
- Upon incoming call, the GMSC must
 - ♦ Analyze MSISDN number
 - ♦ And find MS using the HLR and VLR
- Note: MSISDN structure is not standardized and may vary between providers
 - ♦ Only home-GMSC can correctly interpret it and can therefore correctly pick the right HLR



High Speed Circuit Switched Data



- HSCSD is a GSM standard for "high speed" data communication
 - ♦ No statistical channel sharing with other participants
 - ♦ Supports 28,8 kbit/s
- 1999 Austria by ONE
 - ♦ Special PCMCIA card required
- Obsoleted by GPRS
 - ♦ Main difference: packet switching

General Packet Radio Service (GPRS)

- **GPRS defined by ETSI in late 1997**
 - ♦ Transitional technology towards 3G networks
 - ♦ "GSM Phase 2+" aka "2.5G"
- **Overlaid to GSM network**
 - ♦ Voice and data share same BW and infrastructure
- **Introduces packet switching in a circuit-switched architecture**
- **Regular IP network**
 - ♦ Mobile devices are IP end systems
 - ♦ MTU = 1500 bytes (as usual)
- **Also uses GMSK modulation**

GPRS – Details (1)

- **Different mobile host classes**
 - ♦ Class A: TX & RX of voice & data at the same time
 - ♦ Class B: TX & RX either voice or data but not simultaneously
 - ♦ Class C: User must select either GSM or GPRS network
- **Each GSM time-slot is now a shared resource**
 - ♦ Any mobile host can use it for TX or RX
 - ♦ One mobile host can allocate up to all eight timeslots in the same TDMA frame

GPRS – Details (2)



- **Four different channel coding schemes**
 - ♦ **CS1 (8.8 kbps)**
 - Many FEC bits, used mainly for signalling and upon poor conditions
 - ♦ **CS2 (13.3 kbps)**
 - ♦ **CS3 (15.6 kbps)**
 - Most often used
 - Supports up to 124.8 kbps per 200 kHz channel (=one TDMA frame)
 - ♦ **CS4 (21.4 kbps)**
 - Only few FEC overhead
 - Supports up to 171.2 kbps per TDMA frame
 - Rarely used because of too much retransmissions

GPRS – Details (3)

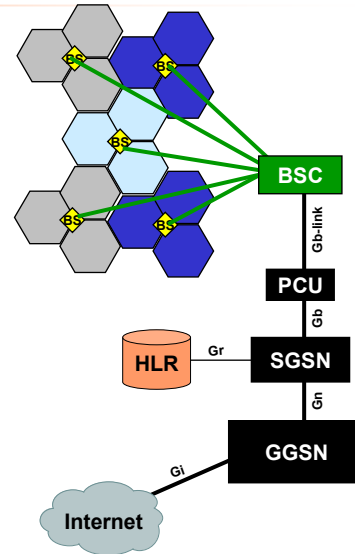


- **Full-duplex communication between mobile host and base station**
 - ♦ But can be asymmetric (different downlink and uplink rates)
- **GSM Association defined 12 "multislot classes" for GPRS**
 - ♦ Each class is associated with a maximum number of uplink and downlink time-slots (per host)
 - "M+N", M...downlink slots, N...uplink slots
 - Class 1 is "1+1", Class 2 is "2+1", ... , Class 12 is "4+4"
 - ♦ Additionally each class has an "active slot constraint" K
 - A host cannot use more than K active slots simultaneously
 - For example, Class 12 has K=5, that is only "4+1", "3+2", "2+3", or "1+4" slots can be used simultaneously

GPRS Support Node (GSN)



- GSN is either a Serving GPRS Support Node (SGSN) or a Gateway GPRS Support Node (GGSN)
- **SGSNs** use Frame Relay (via Gb interface) upstream to Packet Control Units (PCUs)
- **GGSNs** use IP (via Gn interface) downstream to SGSNs and the GPRS Tunneling Protocol (GTP)
 - ♦ Connect GPRS network with a Public Data Network (PDN) via Gi interface
 - Typically PDN = Internet or ATM network
 - ♦ Use AAA services of mobile radio providers



PCU



- **Required to implement GPRS into existing GSM radio devices**
 - ♦ Which only accepts "Transcoder and Rate Adaptation Unit" (TRAU) frames
 - ♦ TRAU frames are used for compressed GSM voice (64 kbit/s => 13 kbit/s)
- **PCU converts SGSN packets into 20 ms PCU frames**
 - ♦ Same duration as TRAU frames
- **Radio Link Control (RLC) layer**
 - ♦ Fragments long data packets into 20 ms chunks
 - ♦ Additionally inserts a sequence number
 - ♦ And a FCS

Enhanced Data for GSM Evolution (EDGE)

- Is an "Enhanced GPRS"
 - ♦ Goal: Higher data-rates
 - ♦ **48 Kbit/s** per channel (typically)
 - ♦ Interim standard towards UMTS
- First implementations
 - ♦ Italy: "TIM Turbo"
 - ♦ Today also in Austria, Switzerland, etc
- Simple upgrade of existing network infrastructure possible

Nine coding schemes

- MCS1-MCS4 use GMSK (like GPRS) and similar radio rates
- MCS5-MCS9 uses the more efficient **8-PSK**
 - ♦ MCS6 supports 29.6 kbps per timeslot
 - ♦ MCS9 supports 59.2 kbps per timeslot
 - ♦ Typically only MCS7 is deployed with all eight slots which results in a (shared) 384 kbps

3GPP



- Maintains standards for UMTS and also GSM
- Founded 4th Dec 1998 by five partners
 - ♦ ARIB (Association of Radio Industries and Businesses, Japan)
 - ♦ ETSI (European Telecommunication Standards Institute)
 - ♦ ATIS (Alliance for Telecommunications Industry Solutions, USA)
 - ♦ TTA (Telecommunications Technology Association, Korea)
 - ♦ TTC (Telecommunications Technology Committee, Japan)
- Technical Standardisation Groups (TSGs)
 - ♦ TSG SA (= Services and Architecture)
 - ♦ TSG CN (= Core Network)
 - ♦ TSG GERAN (= GSM EDGE Radio Access Network)
 - ♦ TSG RAN (= UMTS Radio Access Network)
 - ♦ TSG T (= Terminals)
- Defined ".3gp" files for MMS
 - ♦ Highly compressed videos
 - ♦ Nearly identical with MP4 format
- Don't confuse 3GPP with 3GPP2
 - ♦ 3GPP2 deals with cooperations of companies developing on CDMA2000



<http://www.3gpp.org/>

UMTS



- IMT-2000 standard, maintained by 3GPP
- First UMTS networks
 - ♦ 2001 by Manx Telecom (Isle of Man, Irish Sea)
 - ♦ 2002 (25. Sept) by Mobilkom Austria
 - ♦ 2004 Germany
- 1st phase (Release 1999)
 - ♦ Wideband CDMA
 - ♦ Mobile devices can handle multiple data streams simultaneously



UMTS



- **Frequency Division Duplex (FDD)**
 - ♦ No timeslots, CDMA
 - ♦ BS and MN use different frequencies (downlink 384 kbit/s)
- **Time Division Duplex (TDD, seldom used)**
 - ♦ BS and MN use different (10 ms) timeslots
 - ♦ Timing problems with moving devices and far distances
 - ♦ Up to 2 Mbit/s (theoretically)
- **BS TX Power: typically 20 W**
- **5 MHz channel BW**

CDMA (1) – Basic Concept

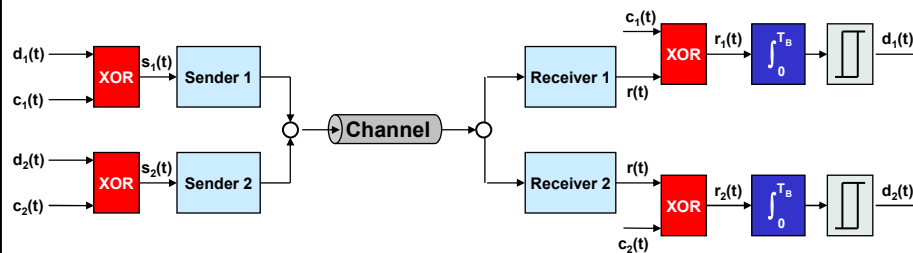


- Code multiplex allows multiple utilization of same frequency channel (without TDM)
- Multiple senders may transmit simultaneously using a different set of **orthogonal code words**
 - ♦ Aka Direct Sequence CDMA (DS-CDMA)
- Each receiver sees the sum of all signals but can extract any particular signal using the sender's code word set
- Number of connections per channel = number of available (orthogonal) codes
 - ♦ Much higher capacities possible compared to time slot techniques (TDMA)
- Alternative method: Frequency Hopping
 - ♦ Requires different ("orthogonal") hopping pattern
 - ♦ Very robust but does not scale to high data rates (< 1-2 Mbit/s with much efforts)

CDMA (2) – Technical Realization



- Transmitter XORs each data bit with a binary code word (CW)
 - Using orthogonal codes, e. g. Walsh codes ("chipping sequence")
 - Results in a BW spreading with a spreading factor SF=length(CW)
- Receiver performs "despreading"
 - 1) XORs received signal with this CW
 - 2) and integrates the result over one bit duration T_B
- For each T_B the orthogonality relation results to
 - Zero if sender and receiver used different CWs
 - One if sender and receiver used same CWs
- Extraction of particular signals works because
 - Spreading, summation of signals, and despreading are *linear* operations

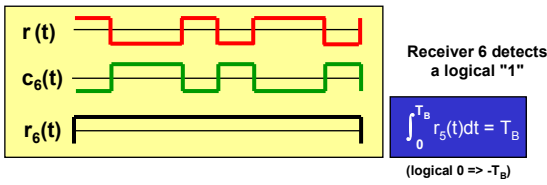
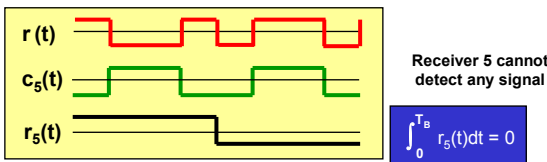
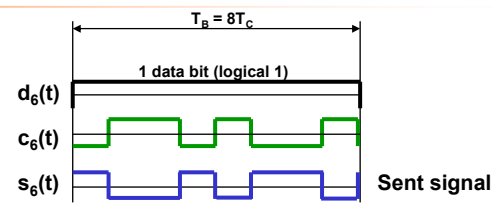


CDMA (3) – Code Example



Example:
Walsh codes of length 8

$c_1 = 00000000$
$c_2 = 00001111$
$c_3 = 00111100$
$c_4 = 00110011$
$c_5 = 01100110$
$c_6 = 01101001$
$c_7 = 01010101$
$c_8 = 01011010$



CDMA (4) – Note



- Walsh codes only work if sent **phase synchronized** – only works downstream
- **Upstream** CDMA communication would require better codes
 - ♦ Whose cross-correlation function is nearly zero for all possible time (=phase) shifts
- A **separate code** set could be used for spreading and channel separation in order to gain an optimal spectral power distribution
- Practical CWs are not 100% orthogonal and cause **additional noise** (reduced SNR at receiver)
 - ♦ SNR does NOT depend on number of CWs!
 - ♦ Only the power levels of other senders are critical
- Therefore each sender should **control its TX power**:
 - ♦ All uplink channels should have same level at base station then the SNR is equal in all channels
 - ♦ The power levels of any downlink channel should be reduced to a minimum (just about receivable) to optimize the SNR in each mobile station

Terms



- **UTRAN – UMTS Terrestrial Radio Access Network**
 - ♦ The UMTS network itself
- **UTRAN consists of**
 - ♦ **Node B (=base station)**
 - ♦ **RNC – Radio Network Controller**
 - Aggregates multiple Node Bs