Robust Remaindering for Real Numbers and Its Applications in Mod Sampling

Xiang-Gen Xia

Department of Electrical and Computer Engineering

University of Delaware

Newark, DE 19716, USA

Email: xxia@ece.udel.edu

献给：南开大学102年周年
陈省身诞辰110周年

Outline

- Introduction
- Robust Chinese Remainder Theorem For Integers
- Robust Chinese Remainder Theorem For Real Numbers
- Mod Sampling
- Conclusion

Remaindering Problem for Integers

- Let N be a large unknown integer and $m_1, m_2, \cdots, m_\gamma$ be γ much smaller moduli
- Let $k_r = N \bmod m_r, \quad r = 1,2,\cdots,\gamma,$ be the γ remainders of N modulo m_r
- In practice, these remainders are measured/observations and may have errors:

$$\widetilde{k}_r = k_r + \Delta k_r$$

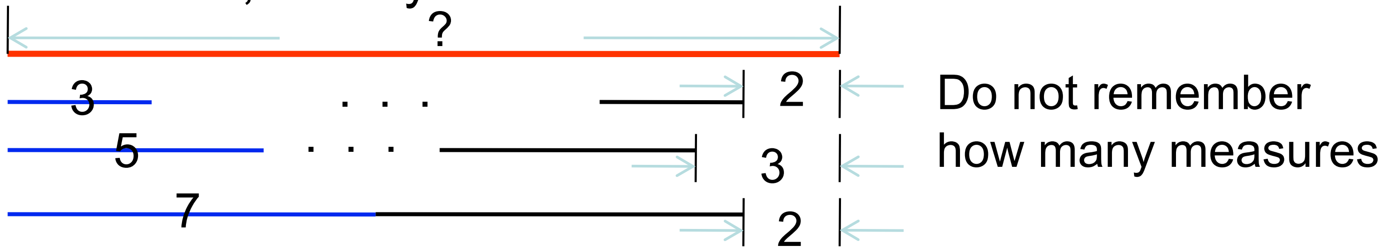
- The question is how to robustly determine N from these erroneous remainders

Chinese Remainder Theorem (CRT)

- In the error-free case of the remainders, CRT provides a solution
- CRT is very fundamental & the best-known original原创 math result contributed from **China**
- CRT has many applications, such as RSA cryptosystem解密算法, secret sharing, distributed storage, fast transform, error correction coding, signal processing etc.

CRT also called Sunzi Theorem

- The following problem was posed by Sunzi in the book *Sunzi Suanjing*: There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?



- The answer is hidden in a Sunzi song named Sunzi Theorem later (also universally known as Chinese Remainder Theorem (CRT)) that gives the conditions necessary for multiple equations to have a simultaneous integer solution:

  He first determined the 'use numbers' 70, 21 and 15 which are multiples of 5*7, 3*7 and 3*5, respectively. Next, he noted that the sum (2*70)+(3*21)+(2*15) equals to 233. Thus 233 is one answer. He then casted out a multiple of 3*5*7 as many times as possible. With this, the least answer, 23, is obtained.

  韩信点兵 **(General Hanxin counting soldiers in Han Dynasty)**

孫子歌 Sunzi Ge

(Sunzi Song in Chinese)

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

- The complete theorem was first given in 1247 by **Qin Jiushao**.

- N can be uniquely determined if and only if

$$0 \leq N < \text{lcm}(m_1, m_2, \cdots, m_\gamma),$$

where lcm stands for the *least common multiple*.

- Under the condition that each pair m_i and m_j for $i \neq j$ are coprime, the solution is given by the following formulas:
  - Let $M = \text{lcm}(m_1, m_2, \cdots, m_\gamma)$,
  - $M_r = M/m_r$,
  - n_r be the number with $1 \leq n_r \leq m_r - 1$ such that

$$n_r M_r = 1 \mod m_r$$

  - then

$$N = \sum_{r=1}^{\gamma} k_{1,r} n_r M_r \mod M$$

n_r is called the multiplicative inverse of $M_r \bmod m_r$, i.e., $n_r = M_r^{-1} \bmod m_r$

- When all m_r, $r = 1, 2, \ldots, \gamma$, are co-prime, $M = m_1 m_2 \cdots m_\gamma$.

- When the moduli m_r are not co-prime, there is a unique solution N modulo M that is the lcm of all the moduli m_r:

$$N = \sum_{\mathrm{r=1}}^{\gamma} k_r\, n_r M_r \text{ mod } M$$

where $M_r = {}^{M}/_{\mu_r}$, n_r is the multiplicative inverse of M_r modulo μ_r, and μ_1, μ_2,…, μ_γ are taken to be any γ pairwise coprime positive integers such that $\prod_{r=1}^{\gamma} \mu_r = M$ and μ_r divides m_r for each $r = 1,2,\ldots,\gamma$,

k_r are the remainders of N mod m_r.

For example, m_1=4, m_2=6; then, M=12; μ_1=4, μ_2=3.

- An example
  - Let $m_1 = 3$, $m_2 = 5$, $N = 14$.
  - $k_1 = N \bmod m_1 = 14 \bmod 3 = 2$,
    $k_2 = N \bmod m_2 = 14 \bmod 5 = 4$.
  - $M = m_1 m_2 = 15$.
  - $M_1 = M / m_1 = 15/3 = 5$, $M_2 = M / m_2 = 15/5 = 3$.
  - $n_1 M_1 = 1 \bmod m_1$ implies $n_1 = 2$; $n_2 M_2 = 1 \bmod m_2$ implies $n_2 = 2$.
  - $N = 2 \cdot 2 \cdot 5 + 2 \cdot 4 \cdot 3 = 44 \bmod 15 = 14$.

CRT is not robust: If $k_1=1$, then $N=4$ and the error is 10.
($\Delta k_1=1$)

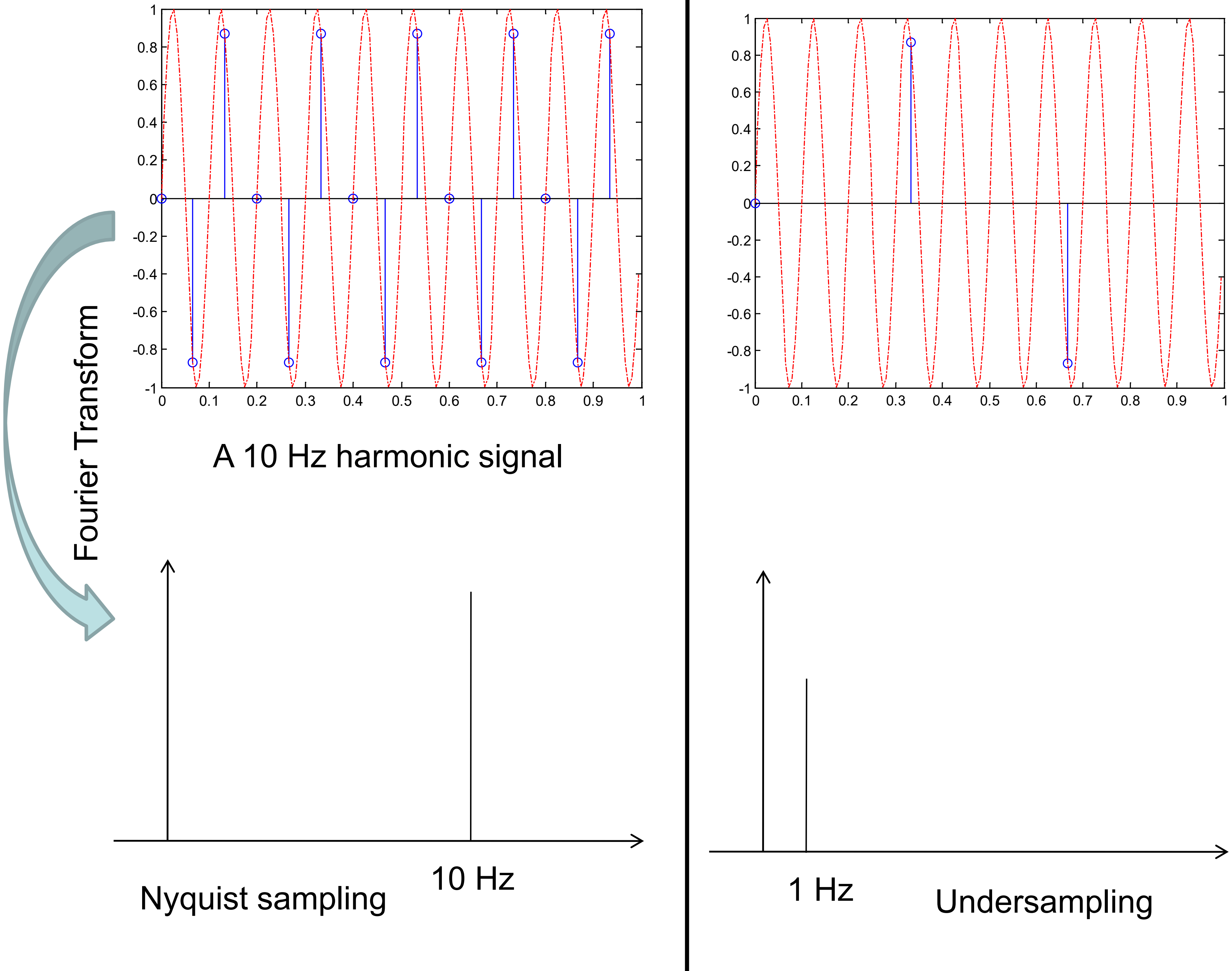
Some of the Existing Works on CRT with Errors

- Most remainders are error free and with probabilistic approaches: Goldreich-Ron-Sudan’2000, Guruswami-Sahai-Sudan’2000
  - With applications in error correction coding
  - Not in the traditional robustness (the solution error level is linear in terms of the input error level)

- Robust CRT: a special case Wang-Wan’1987; and Xia-G. Wang’07, Li-Liang-Xia’09, W. Wang-Xia’10, Xiao-Xia-W.Wang’14
  - Applications in phase unwrapping in SAR imaging of moving targets
  - Robust key generation from wireless channel coefficients

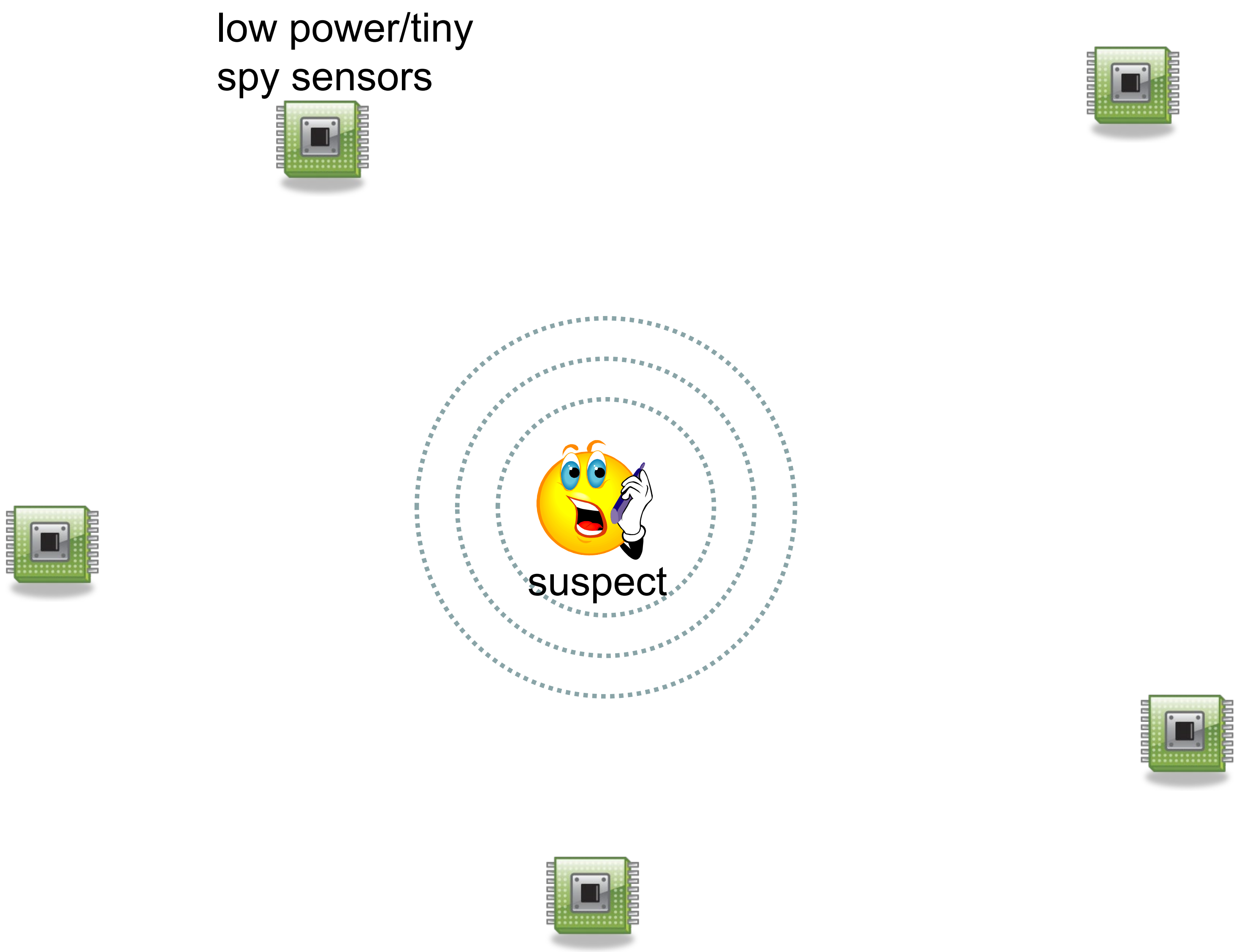
Applications in Signal Processing

- Assume all frequencies of interest are in Hz and of N Hz for integers N. $s(t) = \exp(j2\pi N t)$
- $s[n] = s(nT_s) = \exp(j2\pi N nT_s)$ for some frequency N Hz.
- The sampling frequency $f_s = 1/T_s = m$ has to be N or above to detect the signal frequency N—-Nyquist sampling.
- Assume $m \geq N$. Then, N can be detected by taking the discrete Fourier transform (DFT) of
  $r[n] = s[n] + w[n] = \exp(j2\pi Nn/m) + w[n]$.


Fourier Transform
A 10 Hz harmonic signal
10 Hz
Nyquist sampling
1 Hz
Undersampling

Undersampling

- What happens when $m<N$ called undersampling?
  - N can not be determined.
  - What is detected from the m-point DFT is the remainder of N modulo m called phase wrapping.
  - What can we do in this case? Use multiple samplings!


low power/tiny
spy sensors
suspect

Multiple Undersampling Case with Application in Multiple Low Power Sensors in a Sensor Network

- Why undersampling? Sometimes, the frequency is too large, and/or a device has low power or functionality.
- There are γ low power sensors with low sampling rates.
- There are γ undersampled signals of $s(t)$ of sampling rates m_1Hz, ..., m_γHz with $m_r < N$ from γ low power sensors:

$$s_{m_r}[n] = \exp(j2\pi Nn/m_r), n \in \mathbf{Z},$$

  whose all information is contained in the time period $0 \leq n \leq m_r - 1$.
- By taking the m_r-point DFT of $s_{m_r}[n]$, $n = 0, 1, ..., m_r - 1$, we obtain $k_r = N \bmod m_r$, $r = 1, 2, ..., \gamma$.

- Then, the problem to determine N from the γ undersampled signals $s_{m_r}[n]$ becomes the problem to determine N from γ residues $k_r = N \bmod m_r, r = 1, 2, ..., \gamma$.

This precisely follows the CRT problem!

- In practice, the signal is noisy and these detected remainders from taking the DFTs may have errors. Then, the question is how to determine the large frequency *N* from these erroneous remainders

This precisely follows the robust remaindering problem!

Robust CRT for Integers

- *N* is an integer and $0 < m_1 < m_2 < \cdots < m_\gamma$ are γ moduli and $r_1, r_2, \ldots, r_\gamma$ are the γ remainders of *n*:

$$N = n_i m_i + r_i,\ 0 \le r_i \le m_i - 1,\ 1 \le i \le \gamma,$$

- Let $0 \le \tilde{r}_i \le m_i - 1,\ i = 1,2,\ldots,L,$ be γ erroneous remainders with

$$|\tilde{r}_i - r_i| \le \tau$$

- The **problem** is how to robustly reconstruct *N* from these erroneous remainders.
  - **We need to uniquely determine the folding integers n_i**

Key idea: moduli need to have common divisors (cannot be all pair-wisely co-prime)

For example: $m_i = m\Gamma_i$, and $\{\Gamma_i\}$ are pairwisely coprime

A Closed-Form Solution with Necessary and Sufficient Condition

In the case of error free, **an algorithm to determine the folding integers** n_i

Linear congruences

$L = \gamma$

$$\begin{cases} N = n_1 m_1 + r_1 \\ N = n_2 m_2 + r_2 \\ \vdots \\ N = n_L m_L + r_L \end{cases}$$

take r_1 as a reference and let the last L-1 equations substract the first one →

$$\begin{cases} n_1\Gamma_1 - n_2\Gamma_2 = \dfrac{r_2 - r_1}{m} \triangleq q_{21} \\ n_1\Gamma_1 - n_3\Gamma_3 = \dfrac{r_3 - r_1}{m} \triangleq q_{31} \\ \vdots \\ n_1\Gamma_1 - n_L\Gamma_L = \dfrac{r_L - r_1}{m} \triangleq q_{L1} \end{cases}$$

Bezout's Identity →

$$n_1 = q_{i1}(\Gamma_1)^{-1}_{\text{mod }\Gamma_i} + kq_{i1}\Gamma_i, \; k \in Z$$
$$i = 2, 3, \cdots, \gamma$$

mod Γ_i ↓

$$\begin{cases} n_1 \equiv q_{21}(\Gamma_1)^{-1}_{\text{mod }\Gamma_2} \quad \text{mod } \Gamma_2 \\ n_1 \equiv q_{31}(\Gamma_1)^{-1}_{\text{mod }\Gamma_3} \quad \text{mod } \Gamma_3 \\ \vdots \\ n_1 \equiv q_{L1}(\Gamma_1)^{-1}_{\text{mod }\Gamma_L} \quad \text{mod } \Gamma_L \end{cases}$$

$0 \le n_1 < \Gamma_2\Gamma_3\cdots\Gamma_\gamma$ ←

n_1 is determined by CRT ←

$$n_i = \frac{n_1\Gamma_1 - q_{i1}}{\Gamma_i}$$
$$i = 2, 3, \cdots, \gamma$$

$m_i = m\Gamma_i$, and $\{\Gamma_i\}$ are pairwisely coprime

W.-J. Wang and X.-G. Xia, *IEEE Trans. on Signal Processing*, Nov. 2010.

- When r_i have errors, i.e.,

$$0 \le \tilde{r}_i < m_i \quad \text{and} \quad |\Delta r_i \triangleq \tilde{r}_i - r_i| \le \tau \tag{4}$$

- Estimate q_{i1} in the above algorithm as

$$\hat{q}_{i1} = \left[\frac{\tilde{r}_i - \tilde{r}_1}{m}\right] = q_{i1} + \left[\frac{\Delta r_i - \Delta r_1}{m}\right] \tag{5}$$

- In the above algorithm, we obtain $\hat{n}_i$, $1 \le i \le \gamma$.

$\hat{n}_i = n_i$ for all $1 \le i \le \gamma$, **if and only if**

$\hat{q}_{i1} = q_{i1}$

- Then, each estimated quotient provides a reconstruction $\hat{N}(i) = \hat{n}_i m_i + \tilde{r}_i$, and the average estimation of N is given by

$$\hat{N} = \left[\frac{1}{\gamma}\sum_{i=1}^{\gamma} \hat{N}(i)\right] \tag{6}$$

which is a robust reconstruction of N, i.e., $|N - \hat{N}| \le \tau$. Here, [*] denotes the rounding function

robustness

Theorem 1 (A Necessary and Sufficient Condition)[]

Assume that $m_i = m\Gamma_i$ with Γ_i being pairwise coprime for $1 \le i \le \gamma$, and $0 \le N < \text{lcm}(m_1, m_2, \cdots, m_L)$. Then, $\hat{n}_i = n_i$ for all $1 \le i \le L$, if and only if

$$-m/2 \le \Delta r_i - \Delta r_1 < m/2, \text{ for all } 2 \le i \le \gamma. \qquad (7)$$

Remark: In the algorithm, $\tilde{r}_1$ is used as the reference, which is clearly not necessary. In fact, any remainder can be used as the reference. But a proper reference plays an important role in improving the performance in practice. General studies can be found in the paper below .

Corollary 1[1]

Assume that $m_i = m\Gamma_i$ with Γ_i being pairwise coprime for $1 \le i \le \gamma$, and $0 \le N < \text{lcm}(m_1, m_2, \cdots, m_L)$. If

$$\tau < m/4, \qquad (8)$$

we have $\hat{n}_i = n_i$ for all $1 \le i \le \gamma$.

W.-J. Wang and X.-G. Xia, "A Closed-Form Robust Chinese Remainder Theorem and Its Performance Analysis," *IEEE Trans. Signal Process.*, vol. 58, pp. 5655-5666, Nov. 2010.

如果每个余数的 最大误差 在 所有模的最大公约数 的 四分之一 内 的话，上面的重构是鲁棒的 (如不在内的话就不一定了）

Matrix Modulo Operations and MD-CRT for Integer Vectors

- For a $D \times D$ nonsingular integer matrix M, set $\mathcal{N}$(M) is defined as

  $\mathcal{N}$(M)={k| k=M x, x∈$[0,1)^D$, and integer vector k ∈ $\mathbf{Z}^D$ }

- Matrix modulo operation of an integer vector m

  m = r mod M for r ∈$\mathcal{N}$(M).

  r is called the vector remainder of m modulo M.

- m = Mn+r where r is the vector remainder of m mod M for integer vector n of dimension *D*.
- For multiple matrix moduli $\mathrm{M}_k, \quad k=1,2,...,\gamma,$ integer vector m has multiple vector remainders $\mathrm{r}_k, \quad k=1,2,...,\gamma.$ From these vector remainders, the integer m can be reconstructed by using MD-CRT.

Some Basic Concepts for Integer Matrices

- **Unimodular matrix**: An integer matrix is called unimodular if its determinant is 1 or -1.
- **Divisor**: Integer matrix A is a left divisor of integer matrix M, if $A^{-1}M$ is an integer matrix. Right divisor can be similarly defined.
- **Multiple**: Nonsingular integer matrix A is a left multiple of integer matrix M if A=PM for some integer matrix P.
- **gcld**: Integer matrix A is a common left divisor of integer matrices M and N, if A is left divisor for both M and N. Integer matrix B is called the greatest common left divisor (gcld), if any common left divisor of M and N is a left divisor of B.
- **Co-prime integer matrices**: Two integer matrices M and N are said to be left (right) co-prime if their gcld (gcrd) is unimodular.
- A pair of integer matrices of the same size are more likely co-prime.

Robust MD-CRT for Integer Vectors

- Let non-singular matrix moduli $\mathrm{M}_{\mathrm{k}} = \mathrm{M}\,\Gamma_k$, for an integer matrix M and γ many pairwise commutative and left co-prime integer matrices $\Gamma_k, k = 1,2,\ldots,\gamma$.

- A similar RCRT exists to robustly reconstruct an integer vector from its erroneous vector remainders.

L. Xiao, X.-G. Xia, and Y.-P. Wang, "Exact and Robust Reconstructions of Integer Vectors Based on Multidimensional Chinese Remainder Theorem (MD-CRT)," *IEEE Trans. on Signal Processing*, vol. 68, no. , pp. 5349-5364, Sept. 2020.

Remaindering Problem for Real Numbers/Vectors

- Let R be a large real number, $m_1, \ldots, m_\gamma$ be γ much smaller moduli: one case is $m_i = m\Gamma_i$ for some coprime integers Γ_i, $i = 1, \ldots, \gamma$.
- For $i = 1, \ldots, \gamma$, the remainder of real number R mod m_i is

  $r_i = R \bmod m_i$, i.e., $R = n_i m_i + r_i$,

  where $0 \le r_i < m_i$ and n_i is an integer.

Note: If n_i is not required to be an integer, r_i is always 0.

- The erroneous remainders are $\tilde{r}_i$ with $|\tilde{r}_i - r_i| \le \tau$, $i = 1, \ldots, \gamma$.
- The problem is to robustly reconstruct R from these γ erroneous remainders $\tilde{r}_i$, $i = 1, \ldots, \gamma$.
- It turns out that the previously proposed robust CRT for integers also applies to the above robust real number remaindering problem.

W.-J. Wang and X.-G. Xia, "A Closed-Form Robust Chinese Remainder Theorem and Its Performance Analysis," *IEEE Trans. Signal Process.*, vol. 58, pp. 5655-5666, Nov. 2010.

W.-J. Wang, X.-P. Li, W. Wang, and X.-G. Xia, "Maximum Likelihood Estimation Based Robust Chinese Remainder Theorem for Real Numbers and Its Fast Algorithm," *IEEE Trans. on Signal Processing*, vol. 63, no. 13, pp.3317-3330, July 2015.

Mod Sampling

- Consider a continuous band-limited signal $x(t)$ with bandwidth Ω.
- The voltage range of an ADC is [-Γ/2, Γ/2) for some Γ>0.
- In the conventional ADC, it may be saturated and the sampling is clipping. It is challenging to recover the analog signal from clipped samples.
- **Bhandari-Krahmer-Ramesh** recently proposed the following mod sampling called self-reset (SR) ADC:

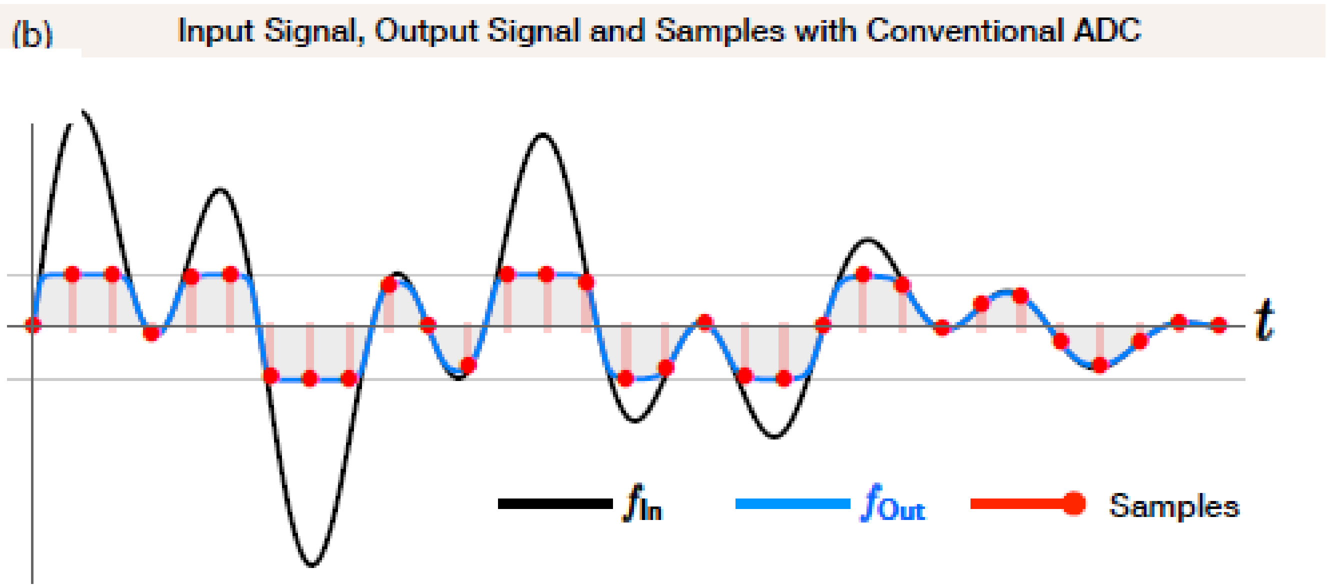
$$\langle x \rangle_\Delta = [x] \bmod \Delta \triangleq x - \Delta \left\lfloor \frac{x}{\Delta} \right\rfloor \in \left[-\frac{\Delta}{2}, \frac{\Delta}{2} \right)$$

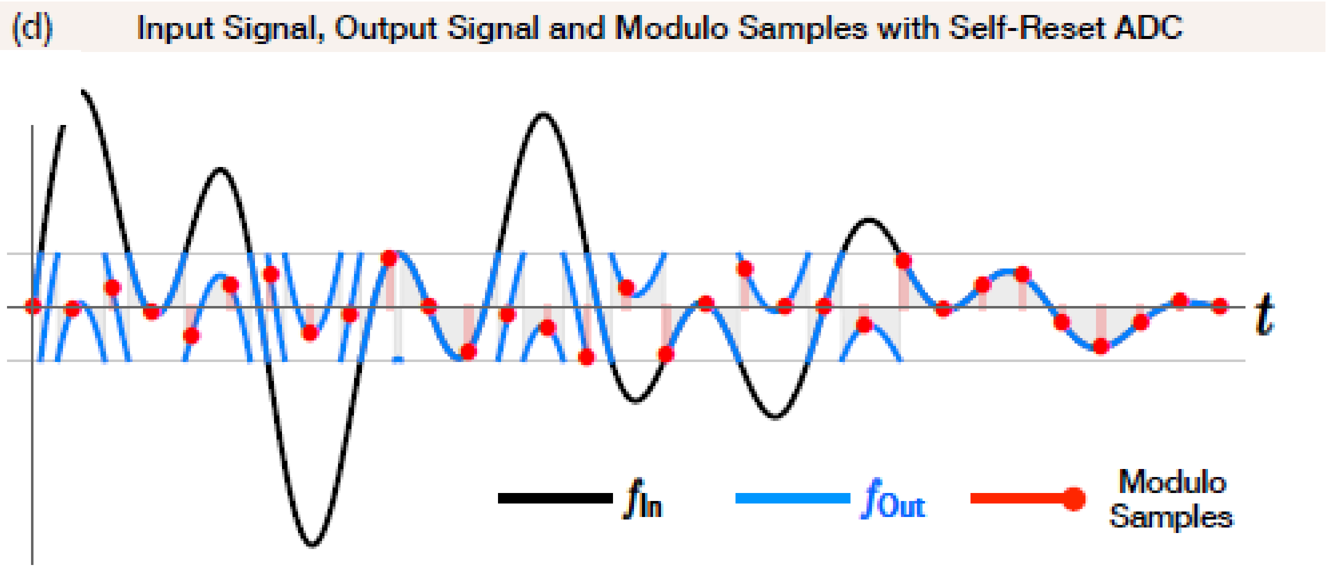
which is equivalent to the real number remaindering:

$$r = x \bmod \Gamma \Leftrightarrow x = n\Gamma + r \text{ for some integer } n$$

where $\Gamma = \Delta$ and $r \in [0, \Gamma)$.

A. Bhandari, F. Krahmer, and R. Raskar, "On unlimited sampling and reconstruction," http://arxiv.org/abs/1905.03901, 2019





A. Bhandari, F. Krahmer, and R. Raskar, “On unlimited sampling and reconstruction,” http://arxiv.org/abs/1905.03901, 2019

Unlimited Sampling

- **Question**: How to recover a band-limited signal from its mod samples $r(nT)= x(nT) \bmod \Gamma$, where T is the sampling interval length?

- **Unlimited Sampling Theorem** [Bhandari-Krahmer-Ramesh]:

  When the sampling interval length $T<1/(2e\Omega)$, a band-limited signal with bandwidth Ω can be reconstructed from its mod samples (or self-reset ADC).

- Although the reconstruction is possible from the mod samples, its sampling rate is about 17 times faster than the Nyquist sampling rate, which may be too high in some applications.

A. Bhandari, F. Krahmer, and R. Raskar, "On unlimited sampling and reconstruction," http://arxiv.org/abs/1905.03901, 2019

Signal Reconstruction from Mod Sampling Using Robust CRT for Reals

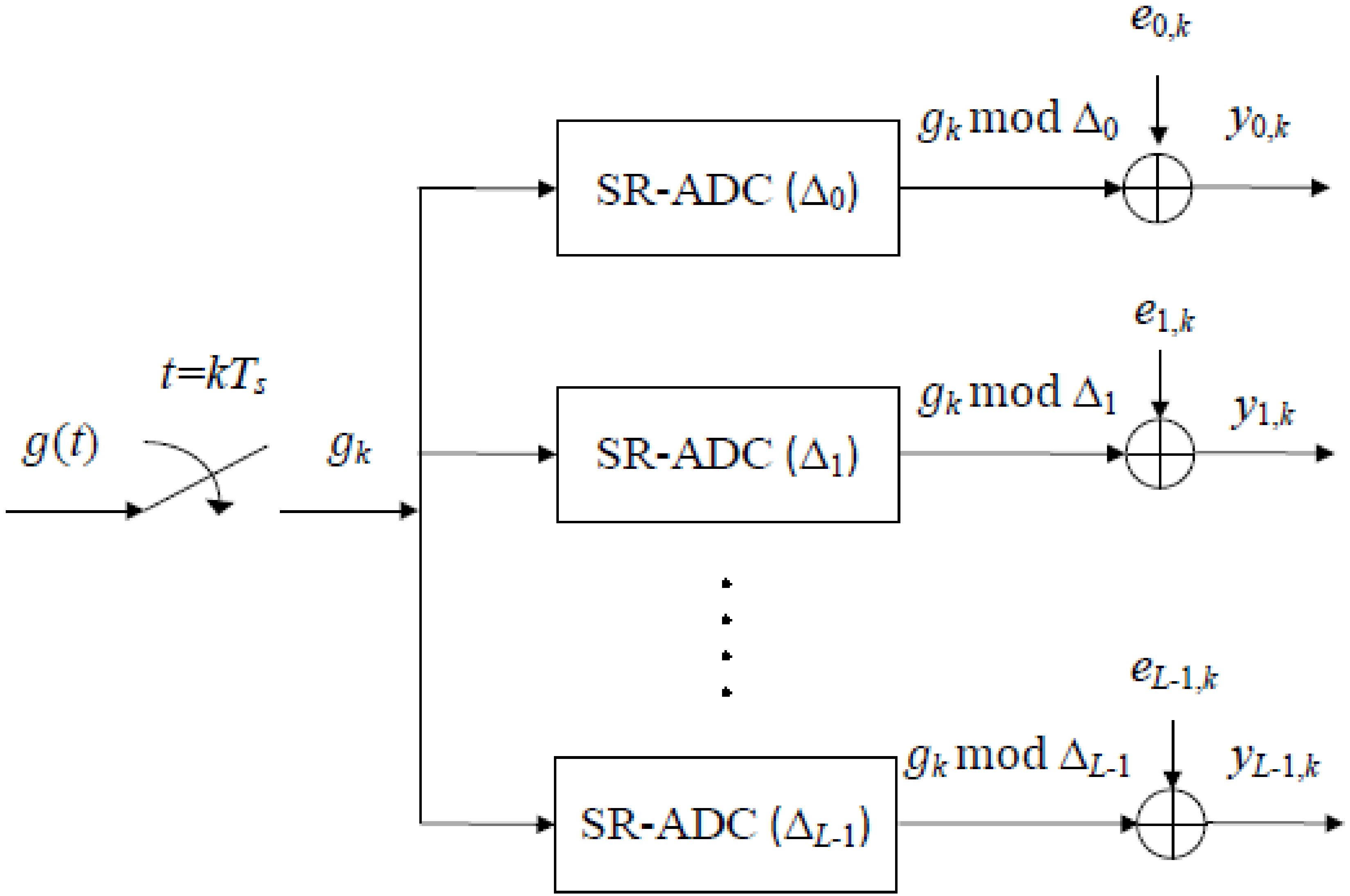
- **Lu Gan (@Brunel Univ.) and Hongqing Liu** recently proposed to reconstruct a signal value from multiple ADC mod samples:

  $r_i(kT) = x(kT) \bmod \Gamma_i, i = 1,2,\ldots,\gamma,$

  where Γ_i are ADC voltage ranges.
- Let m be a common real number so that $\Gamma_i := m\Gamma_i$, and $\Gamma_i, i = 1,2,\ldots,\gamma$, are co-prime integers.
- Then, for each time k, the reconstruction $x(kT)$ from its γ mod samples $r_i(kT) = x(kT) \bmod \Gamma_i, i = 1,2,\ldots,\gamma$, coincides with the robust CRT for real numbers described before, where a signal usually has noise, i.e., the remainders are erroneous.
- The sampling rate is the Nyquist sampling rate, and does not have to higher than the Nyquist rate.

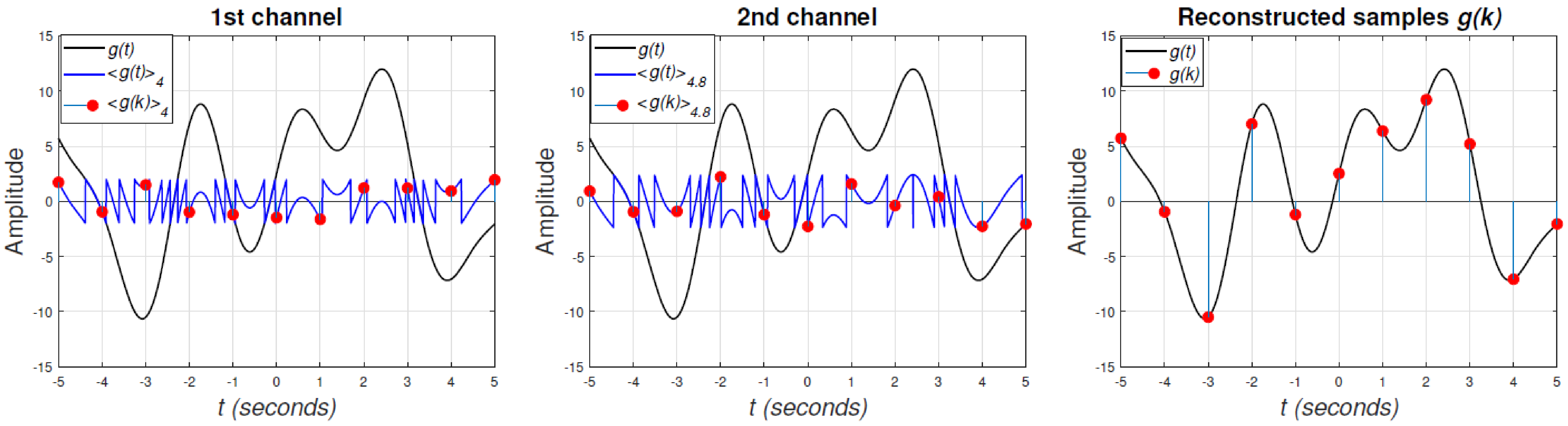
L. Gan and H. Liu, "High dynamic range sensing using multi-channel modulo samplers," in *Proc. IEEE 11th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hangzhou, China., Jun. 2020. For real valued signals

Y. Gong, L. Gan, and H. Liu, "Multi-channel modulo samplers constructed from Gaussian integers," *IEEE Signal Processing Letters*, to appear. For complex valued signals



L. Gan and H. Liu, "High dynamic range sensing using multi-channel modulo samplers," in *Proc. IEEE 11th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hangzhou, China., Jun. 2020. For real valued signals

Y. Gong, L. Gan, and H. Liu, "Multi-channel modulo samplers constructed from Gaussian integers," *IEEE Signal Processing Letters*, to appear. For complex valued signals

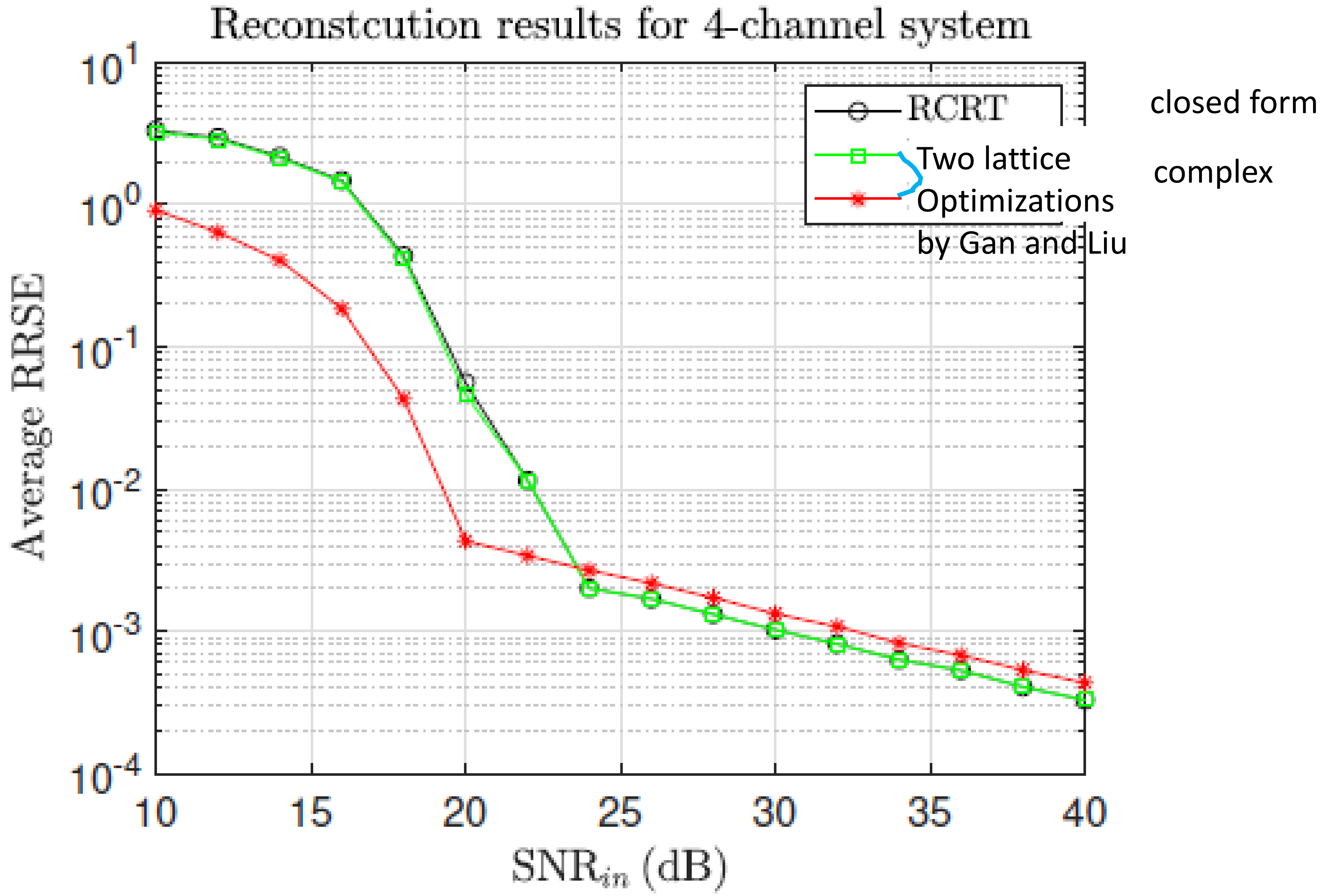


(a) (b) (c)

An example of digitizing $x(t)$ with a 2-channel SR-ADC system. Here, $m = 0.8$, $\Delta_0 = 0.8 \cdot 5 = 4$ and $\Delta_1 = 0.8 \cdot 6 = 4.8$. The Nyquist sampling period is $1\, s$. (a) and (b) show the outputs of the 1st and the 2nd channels, respectively. (c) shows the reconstructed values

Note that all the real *m*, real moduli, and real sampling interval lengths can be properly made integers in order to apply robust CRT.

L. Gan and H. Liu, “High dynamic range sensing using multi-channel modulo samplers,” in *Proc. IEEE 11th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hangzhou, China., Jun. 2020.



L. Gan and H. Liu, "High dynamic range sensing using multi-channel modulo samplers," in *Proc. IEEE 11th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Hangzhou, China., Jun. 2020.

Generalization of Vector-Valued Bandlimited Signals with Matrix Mod Sampling

- Vector-valued bandlimited signal $\mathbf{x}(t)=[x_1(t),\ldots,x_D(t)]^T$ if every function $x_d(t)$ of vector components is bandlimited.
- Vector self-reset (VSR) ADC: x=Mn+r, where x is x=x(*kT*) for some integer *k* and *T* is the sampling interval length in the time domain, r is the vector remainder of x mod M and n is a unknown integer vector.
- Open Questions:

  1) What will happen to the unlimited sampling theorem by properly choosing the modulo matrix M?

  2) Can it do better than the individual SR ADC unlimited samplings? i.e., can it have lower sampling rates than that for the individual unlimited samplings?
- When all the vector component signals are the same, the multiple SR ADC proposed by Gan et al can be thought of as a vector SR by using a diagonal modulo matrix M=diag($M\Gamma_1, \ldots, M\Gamma_\gamma$). In this case, the sampling rate can be just the Nyquist rate.

Multi-VSR ADC for Vector-Valued Real Signals or ADC for Complex-Valued Signals

- **Gong, Gan, and Liu** proposed multiple SR-ADC for complex-valued signals that is equivalent to multiple VSR for vector-valued real signals of dimension 2
- Two co-prime modulo matrices $\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}, \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}$
  - The maximal signal value **<12.5**, while for two comparable individual real SR ADC for each component, the maximal signal value **<10**.
- Three co-prime modulo matrices $\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}, \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$
  - The maximal signal value **<50**, while for three comparable individual real SR ADC for each component, the maximal signal value **<30**.
- Four co-prime modulo matrices $\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}, \begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ -4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -4 \\ 4 & 1 \end{pmatrix}$
  - The maximal signal value **<212.5**, while for four comparable individual real SR ADC for each component, the maximal signal value **<30**.
- Vector VSR ADC may perform better than scalar SR ADC.
  - One of the main reasons why the dynamic range of MD CRT may be better than the dynamic range of independent 1D CRT is that there are much more choices of co-prime MD integer matrices than that of co-prime integers.

Y. Gong, L. Gan, and H. Liu, "Multi-channel modulo samplers constructed from Gaussian integers," *IEEE Signal Processing Letters*, to appear. For complex valued signals

A Possible Systematic Method to Construct Co-Prime Commutative Integer Modulo Matrices in MD-RCRT

- Use co-prime algebraic integers and their corresponding integer matrix representations

- **A question**: The commutativity of integer modulo matrices is too strong. Can the MD-RCRT be generalized to non-commutative integer modulo matrices?

Conclusion

- We have introduced robust CRT for both integers and real numbers.
  - This topic has been extended to many general versions
    - general moduli
    - multi-stage robust CRT
    - two large integers reconstruction from their remainder sets
    - polynomials with applications in error correction coding
    - vector versions with integer matrix moduli
  - It has applications in phase unwrapping in SAR imaging of moving targets and error control coding etc.
  - New applications will be interesting.

- More studies on bandlimited signal reconstruction from mod samplings using robust CRT for real numbers and vectors may be interesting.

Some References on CRT

- Li Xiao, X.-G. Xia, and Y.-P. Wang, Exact and Robust Reconstructions of Integer Vectors Based on Multidimensional Chinese Remainder Theorem (MD-CRT*), IEEE Transactions on Signal Processing*, vol. 68, pp. 5349-5364, Sept. 2020.
- X.-P. Li, T.-Z. Huang, Q. Liao, and X.-G. Xia, Optimal Estimates of Two Common Remainders for A Robust Generalized Chinese Remainder Theorem, *IEEE Transactions on Signal Processing*, vol. 67, no. 7, pp. 1824-1837, Apr. 1, 2019.
- L. Xiao and X.-G. Xia, Robust Polynomial Reconstruction via Chinese Remainder Theorem in the Presence of Small Degree Residue Errors, *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 11, pp. 1778-1782, Nov. 2018.
- L. Xiao and X.-G. Xia, Frequency determination from truly sub-Nyquist samplers based on robust Chinese remainder theorem, *Signal Processing*, vol. 150, pp. 248-258. Sept. 2018.
- L. Xiao and X.-G. Xia, Minimum degree-weighted distance decoding for polynomial residue codes with non-pairwise coprime moduli, *IEEE Wireless Communications Letters*, vol. 6, no. 4, pp. 558-561, Aug. 2017.
- L. Xiao, X.-G. Xia, and H. Y. Huo, Towards Robustness in Residue Number Systems, *IEEE Transactions on Signal Processing*, vol. 65, no. 6, pp. 1497-1510, Mar. 2017.
- X.-P. Li, X.-G. Xia, W. J. Wang, and W. Wang, A robust generalized Chinese remainder theorem for two Integers, *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7491-7504, Dec. 2016.
- L. Xiao, X.-G. Xia, and H. Y. Huo, New Conditions on Achieving the Maximal Possible Dynamic Range for a Generalized Chinese Remainder Theorem of Multiple Integers, *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2199-2203, Dec. 2015.
- W.-J. Wang, X.-P. Li, W. Wang, and X.-G. Xia, Maximum Likelihood Estimation Based Robust Chinese Remainder Theorem for Real Numbers and Its Fast Algorithm, *IEEE Trans. on Signal Processing*, July 2015.
- L. Xiao and X.-G. Xia, Error Correction in Polynomial Remainder Codes with Non-Pairwise Coprime Moduli and Robust Chinese Remainder Theorem for Polynomials, *IEEE Trans. on Communications*, vol. 63, no. 3, pp.605-616, March 2015.
- W. Wang, X.-P. Li, X.-G. Xia, and W.-J. Wang, The largest dynamic range of a generalized Chinese remainder theorem for two integers, *IEEE Signal Processing Letters*, vol. 22, no. 2, pp. 254-258, Feb. 2015.
- L. Xiao, X.-G. Xia, and W.-J. Wang, Multi-stage robust Chinese remainder theorem, *IEEE Trans. on Signal Processing*, vol. 62, no. 18, pp. 4772-4785, Sept. 2014.
- L. Xiao and X.-G. Xia, A Generalized Chinese Remainder Theorem for Two Integers, *IEEE Signal Processing Letters*, vol. 21, no. 1, pp. 55-59, Jan. 2014.
- W.-J. Wang and X.-G. Xia, A closed-form robust Chinese remainder theorem and its performance analysis, *IEEE Trans. on Signal Processing*, Nov. 2010.
- X.-W. Li and X.-G. Xia, Location and Imaging of Elevated Moving Target Using Multi-Frequency Velocity SAR with Cross-Track Interferometry, *IEEE Trans. on Aerospace and Electronic Systems*, vol. 47, April 2011.
- X.-W. Li and X.-G. Xia, A Robust Doppler Ambiguity Resolution Using Multiple Paired Pulse Repetition Frequencies, *IET Radar, Sonar & Navigation*, vol. 4, pp. 375-383, June 2010.
- X.-W. Li, H. Liang, and X.-G. Xia, A Robust Chinese Remainder Theorem with its Applications in Frequency Estimation from Undersampled Waveforms, *IEEE Trans. on Signal Processing*, Nov. 2009.
- H. Liang, X.-W. Li, and X.-G. Xia, Adaptive Frequency Estimation with Low Sampling Rates Based on Robust Chinese Remainder Theorem and IIR Notch Filter, *Advances in Adaptive Data Analysis*, vol. 1, no. 4, pp. 587-600, Oct. 2009.
- X.-W. Li and X.-G. Xia, A Fast Robust Chinese Remainder Theorem Based Phase Unwrapping Algorithm, *IEEE Signal Processing Letters*, vol.15, pp.665-668, Oct. 2008.

- G. Li, H. Meng, X.-G. Xia, and Y.-N. Peng, Range and Velocity Estimation of Moving Targets Using Multiple Stepped-frequency Pulse Trains, *Sensors*, vol. 8, pp.1343-1350, Feb. 2, 2008.
- G. Li, J. Xu, Y. Peng, and X.-G. Xia, Location and imaging of moving targets using non-uniform linear antenna array, *IEEE Trans. on Aerospace and Electronic Systems*, vol. 43, July 2007.
- G. Li, J. Xu, Y. Peng, and X.-G. Xia, Moving target location and imaging using dual-speed velocity SAR, *IET Radar, Sonar & Navigation*, vol. 1, no. 2, pp.158-163, April 2007.
- G. Li, J. Xu, Y. Peng, and X.-G. Xia, An efficient implementation of a phase unwrapping algorithm, *IEEE Signal Processing Letters,* June 2007.
- H. Liao and X.-G. Xia, A Sharpened Dynamic Range of a Generalized Chinese Remainder Theorem for Multiple Integers, *IEEE Trans. on Information Theory,* Jan. 2007.
- X.-G. Xia and G. Wang, Phase Unwrapping and A Robust Chinese Remainder Theorem, *IEEE Signal Processing Letters,* April 2007.
- X.-G. Xia and K. Liu, A Generalized Chinese Remainder Theorem for Residue Sets with Errors and Its Application in Frequency Determination from Multiple Sensors with Low Sampling Rates, *IEEE Signal Processing Letters*, Nov. 2005.
- G. Wang, X.-G. Xia , V. C. Chen, and R. L. Fiedler, Detection, Location and Imaging of Fast Moving Targets Using Multi-Frequency Antenna Array SAR, *IEEE Trans. on Aerospace and Electronics Systems,* vol. 40, pp.345-355, Jan. 2004.
- X.-G. Xia, An efficient frequency estimation algorithm from multiple undersampled waveforms, *IEEE Signal Processing Letters,* Feb. 2000.
- G. Zhou and X.-G. Xia , Multiple frequency detection in undersampled complex-valued waveforms with close multiple frequencies, *IEE Electronics Letters,* vol.33, no.15, pp.1294-1295, July 1997.
- X.-G. Xia, On estimation of multiple frequencies in undersampled complex valued waveforms, *IEEE Trans. on Signal Processing* , Dec. 1999.

Thank You!