

# 适用多种码速率的遥控副载波数字化解调设计

沈小虎, 王翠莲, 周东

(北京空间飞行器总体设计部, 北京 100094)

**摘要:** 统一 S 波段测控体制采用相位调制技术实现遥控副载波的调制, 星上应答机在实现 S 波段载波剥离后将遥控副载波送给星上遥控设备进行解调最终实现指令和数据的上注; 遥控设备通常采用模拟电路实现解调, 当输入不同码速率时均需要重新调试输入滤波器, 并且当码速率较低时调试困难, 滤波器及解调环路的工作参数更容易受环境温度影响, 导致解调损失变高, 跟踪解调环路易失锁; 文章介绍了一种适应多种码速率的遥控副载波数字化解调方法; 可以有效解决上述问题, 减小解调损失, 提高产品可靠性; 文章中涉及到了数字化副载波跟踪环设计, 数字化自动增益控制以及早迟路位同步恢复环路的设计方法, 最后提出了两种提高产品可靠性的设计措施; 本方法适用于采用 FPGA 工程实现, 具有解调损失小, 节省资源易实现以及可靠性高等优点。

**关键词:** 遥控副载波; 数字化解调; 科斯塔斯环

## Remote Sub-carrier Digital Demodulation for Multiple Code Rates

Shen Xiaohu, Wang Cuilian, Zhou Dong

(Institute of Spacecraft System Engineering, Beijing 100094, China)

**Abstract:** Unified S-Band transponder tracks phase modulate carrier and exports remote sub-carrier which is PSK signal. Remote control unit receives sub-carrier and demodulates PSK signal by analog circuit. It is a hard work to debug a very small bandwidth band pass filter when the bit rate is very low also the parameter of band pass filter is changed when undergo large range temperature fluctuate. Once the designed parameter of filter is changed that may led to high loss of demodulation and easy to unlock. This paper presents a digital demodulation method which can avoid the shortcoming of analog circuit and improve the reliability of the product. The key technologies are digital carrier tracking, auto gain control and early-late bit synchronization. This method is suitable for the implementation of the project using the FPGA. It has the advantages of low demodulation loss, saving resources, easy realization and high reliability.

**Keywords:** remote sub-carrier; digital demodulation; Costas loop

## 0 引言

传统遥测遥控体制上行信号采用相位调制 (PM) 方式, 主载波信号上调制了多种频率的测距音信号以及上行 8 kHz 的遥控副载波。其中测距音信号用来实现星地测距测速功能, 遥控副载波采用 PSK 调制方式实现遥控指令与上行注入数据的发送。星上应答机滤除上行载波后将测距信号调制在下行载波上转发, 对遥控副载波信号进行低通滤波后送后续遥控设备进行解调。传统遥控解调电路采用模拟锁相环路实现 8K 副载波的跟踪解调输出 PCM 数据。但是模拟解调电路有自身的缺点, 由于副载波跟踪环路采用的是简单的锁相跟踪环, 所以对前置滤波器的滤波性能要求较高, 否则跟踪环路的环内信噪比低容易失锁, 滤波器的带宽要根据信息码速率来调整, 当遥控码速率较低情况下很难将滤波器的带宽调试的较窄, 并且较窄的滤波器环路参数更容易受环境温度的影响而发生参数漂移。深空探

测任务由于通信距离遥远, 常采用低码速率通信, 当码速率低于 500 bps 以下时滤波器调试将会变得十分困难。采用数字化解调方法可以解决上述问题。应答机输入给遥控设备的副载波信号特征如下:

- 1) 调制方式: PSK 调制;
- 2) 输入信号功率 (信号加噪声) 的有效值: 500 ~ 1100 mV;
- 3) 输入信号  $E_b/N_0$ : 大于 16 dB;
- 4) 输入信号码速率: 125 bps、250 bps、500 bps;
- 5) 副载波频率准确度:  $8000 \text{ Hz} \pm 0.02\%$ ;
- 6) 位同步时间: 小于 128 位;
- 7) 误码率: 遥控解调器误码率小于  $5 \times 10^{-6}$ 。

遥控解调器接收应答机输入的 PSK 调制信号首先经过模拟带通滤波器, 滤除带外噪声信号, 为了适应最高 500 bps 的码速率, 模拟带通滤波器带宽统一设计为 1.2 kHz。经过滤波后按照 64 kHz 的采样速率进行 8 位 A/D 量化, 随后送 FPGA 进行解调处理。采用数字解调技术, 以前模拟解调电路上的带通滤波器的主要功能转变为了抗混叠滤波, 所以三种码速率可以采用一个滤波器来适应, 更多的噪声

收稿日期: 2018-11-06; 修回日期: 2018-12-04。

作者简介: 沈小虎 (1974-), 男, 北京人, 硕士研究生, 主要从事星载测控通信产品研制方向的研究。

滤除工作放在了 FPGA 内部实现。图 1 是 FPGA 内部副载波跟踪环路框图，输入信号分为同相、正交分量与本地 NCO 相乘实现下变频，随后进行自动增益控制保证输入给后续运算电路的信号功率稳定。支路滤波器采用滑动平均加抽取的方法对信号中的高频分量进行滤除。鉴相器输出鉴相误差经过环路滤波器后控制 NCO 调整本地频率及相位使之与输入 8 kHz 副载波同频同相实现跟踪。

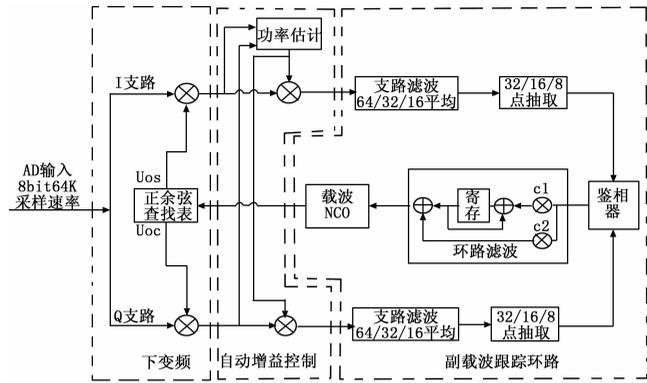


图 1 数字解调副载波跟踪环 FPGA 设计框图

## 1 副载波解调器及算法描述

### 1.1 下变频及环路参数

令输入 PSK 信号为：

$$U_i(t) = \sqrt{2}aD(t)\sin(\omega_i t + \theta_i) + n \quad (1)$$

其中： $D(t)$  表示调制数据， $\sqrt{2}a$  表示信号幅度， $n$  表示方差为  $\sigma^2$  的高斯白噪声；

与本地输出的同相正交支路载波相乘后输出的信号为：

$$\text{本地同相: } U_{os}(t) = \sqrt{2}b\sin(\omega_o t + \theta_o);$$

$$\text{本地正交: } U_{oc}(t) = \sqrt{2}b\cos(\omega_o t + \theta_o);$$

$$i_p(t) = U_i(t) \times U_{os}(t) = -abD(t)[\cos((\omega_i + \omega_o)t + (\theta_o + \theta_i)) - \cos(\omega_e t + \theta_e)] + n_{i,p}$$

其中： $\omega_e = \omega_i - \omega_o$ ； $\theta_e = \theta_i - \theta_o$ 。

公式中，角速度和频项为高频分量，差频项为低频分量。对于输入信号  $U_i(t)$  功率为  $a^2$ ，噪声功率为  $\sigma^2$ ，输入信噪比为  $smr = a^2/\sigma^2$ ，当输入信号在同相支路上与复制载波  $U_{os}(t)$  相乘后，可以计算出噪声项  $n_{i,p}$  的功率仍旧维持在  $\sigma^2$ 。混频后再经过支路低通滤波后滤除了倍频分量与带外噪声得到了如下混频结果：

$$I_p(t) = abD(t)\cos(\omega_e t + \theta_e) + n_i \quad (2)$$

$$Q_p(t) = abD(t)\sin(\omega_e t + \theta_e) + n_q \quad (3)$$

支路低通滤波器滤除下变频后其中的高频分量及噪声再进行鉴相。鉴相器的输出反映了输入副载波与本地 NCO 输出副载波的相位差，当相差为正时，表示本地 NCO 输出信号相位滞后输入信号则加快本地 NCO 频率，否则减慢本地 NCO 频率。鉴相器有多种形式，表 1 总结了四种鉴相器算法<sup>[1]</sup>。

其中第一种方法计算量大，需要采用 CORDIC 算法来

实现，第二种方法需要设计除法运算电路，相比较来看只有第四种实现起来简单，适合资源较少的反熔丝型 FPGA 来实现，但缺点是鉴相结果受输入信号幅度影响。正是考虑到这一点所以在信号路径上需要增加自动增益控制环节。

表 1 常用鉴相算法

鉴相器算法	算法描述
$\theta_e = \arctan(Q_p/I_p)$	鉴相结果与信号幅度无关，运算量大
$\theta_e = Q_p/I_p$	近似计算 $\arctan(Q_p/I_p)$ ，当 $\theta_e$ 较小时与 $\tan(\theta_e)$ 近似
$\theta_e = Q_p \times I_p$	近似计算 $\sin(2\theta_e)$ ，当 $\theta_e$ 较小时 $\sin(2\theta_e)$ 与 $2\theta_e$ 近似
$\theta_e = Q_p \times \text{sign}(I_p)$	$\text{sign}(\cdot)$ 是符号函数，计算量最小，鉴相结果与 $\sin(\theta_e)$ 成正比，与信号幅度相关

### 1.2 支路滤波器设计

支路滤波器采用滑动累加求平均再抽取的方法实现。滑动平均相当于低通滤波器。当码速率为 500 bps 时采用 16 点滑动平均 8 点抽取，相当于经过截止频率为 4 kHz 的低通滤波器，抽取后鉴相器的更新频率是 8 kHz；当码速率为 250 bps 时采用 32 点平均 16 点抽取，相当于经过截止频率是 2 kHz 的低通滤波，抽取后鉴相器的更新频率是 4 kHz；当码速率为 125 bps 时采用 64 平均 32 点抽取，相当于 1 kHz 的低通滤波，鉴相器的更新频率是 2 kHz。

### 1.3 自动增益控制设

应答机输入给遥控设备信号的有效值在 500~1100 mv RMS 波动，通过自动增益动态调整输入信号的放大量可以使输入信号保持稳定的幅值，有利于基带处理避免过载并充分利用量化比特，减小量化误差。自动增益模块对下变频后信号进行功率估计，并与目标值比较，刷新补偿因子，实现对输入信号的动态放大。算法采用前向调整的方式，没有反馈路径，图 2 是该算法的实现框图<sup>[2]</sup>。

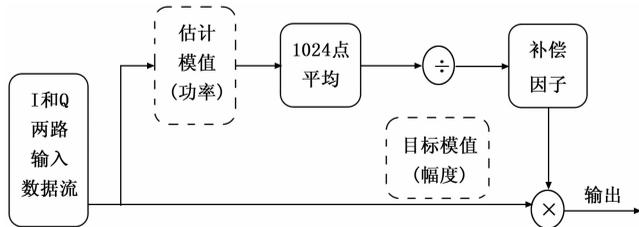


图 2 自动增益控制模块实现方法

输入信号功率不会有太快的波动，采用 1024 个采样数据滑动求平均来估计出当前的功率，并计算出补偿因子，计算功率估计时可以采用如下近似计算方法实现<sup>[3]</sup>。

$$\sqrt{I^2 + Q^2} \approx \max(|I|, |Q|) + \frac{1}{2} \min(|I|, |Q|) \quad (3)$$

### 1.4 环路滤波器设计

副载波跟踪环的环路滤波器采用理想二阶环，可以对

频率阶跃信号无误差的跟踪。环路滤波器的实现形式如图 1 所示, 滤波器包括积分支路与直通支路, 令:  $t_s$  是环路鉴相误差更新频率;  $\epsilon$ : 是环路阻尼系数;  $b_l$ : 环路带宽, 则环路无阻尼振荡频率:

$$\omega_n = (8 \times \epsilon \times b_l) / (4 \times \epsilon^2 + 1) \quad (4)$$

令:  $K = K_a \times K_b$  环路增益,  $K_a$ : 鉴相增益,  $K_b$ : 压控增益;  $P$ : 自动增益控制设定的输出信号幅度。  $f_s$ : 数控振荡器 (NCO) 的工作频率,  $nco\_len$ : NCO 的累加位宽; 则:  $K_a = 2P/\pi, K_b = 2 \times \pi \times f_s / 2^{nco\_len}$ ; 则锁相环路积分支路<sup>[4]</sup>:

$$C_1 = \frac{1}{K} \frac{4 \times t_s \times \omega_n^2}{4 + 4 \times \epsilon \times \omega_n \times t_s + (\omega_n \times t_s)^2} \quad (5)$$

直通支路:

$$C_2 = \frac{1}{K} \frac{8 \times \epsilon \times \omega_n}{4 + 4 \times \epsilon \times \omega_n \times t_s + (\omega_n \times t_s)^2} \quad (6)$$

### 1.5 位同步环路设计

位同步环路的主要功能是提取调制数据的位同步信息, 恢复出本地 PCM 码流时钟信号。采用早准支路的方法实现位同步时钟的恢复。位同步环路的输入是图 1 中同相支路的滤波器的输出, 图 3 是位同步环路 FPGA 实现框图<sup>[5]</sup>。

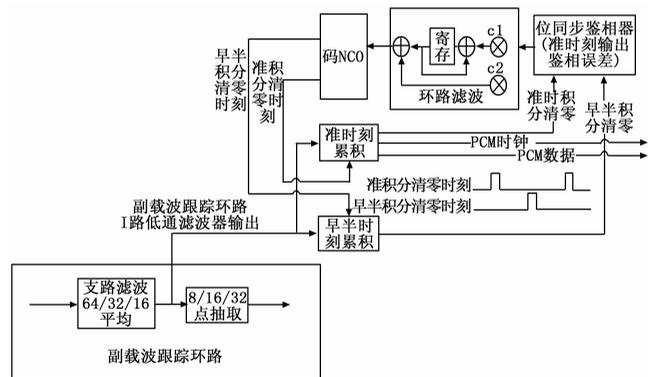


图 3 位同步环路 FPGA 设计框图

码 NCO 根据信息码速率, 输出相应频率的准时刻积分清零脉冲以及相差  $\pi$  相位的早半积分清零脉冲。图 3 中, “准时刻累积” 模块对输入信号进行积分累加, 当准积分清零时刻到达时输出累加值, 同时将自身累加值清零。“早半时刻累积” 模块依据早半积分清零脉冲输出累加值以及对累加器清零。位同步鉴相器在准积分清零时刻依据两个积分清零值按照如下鉴相算法<sup>[6]</sup>计算出位同步的鉴相误差, 并输出给环路滤波器。

令:  $I_p(n), I_p(n-1), I_c(n), ph_e$  分别是准时刻当前积分清零值、准时刻上一次积分清零值, 早半时刻当前积分清零值以及相位误差, 则鉴相器的计算规则是, 如果:  $sign(I_p(n)) = sign(I_p(n-1))$ ; 则:  $ph_e = 0$ ; 如果:  $I_p(n-1) > 0$  并且  $I_p(n) < 0$ ; 则:  $ph_e = -I_c(n)$ ; 如果:  $I_p(n-1) < 0$  并且  $I_p(n) > 0$ ; 则:  $ph_e = I_c(n)$ ;

位同步环的环路滤波器与载波环的环路滤波器有相同

的参数定义, 所不同的是, 位同步环路的鉴相增益和环路鉴相更新频率。令:  $f_b$  是遥控信息码速率则:  $K_a = P/\pi, t_s = 1/f_b$ 。位同步环路中直通与积分支路的系数计算方法与副载波跟踪环计算方法一致。当位同步环路实现锁定时, 此时的准积分清零时刻脉冲即是恢复出来的 PCM 时钟。当采用硬判决实现解调时, 则当准时刻积分清零值为正数则解调输出 1, 否则输出 0。由于副载波跟踪环的稳定平衡点为  $0^\circ$  或  $180^\circ$  所以导致解调输出的数据存在相位模糊度, 即原始信息位如果是 0 则解调后全部输出 1, 原始信息为是 1 则解调输出全为 0。信息位的相位解模糊由后续帧同步检测电路根据特定的数据帧内容进行识别。

### 2 工程参数设计

副载波跟踪环路参数设计步骤如下: 首先确定 AGC 输出功率  $P = 2048$  (依据下变频后数据输出位宽决定), 其次确定三种码速率下不同的副载波跟踪环路带宽,  $b_l = 10 \text{ Hz}_{125 \text{ bps}}, b_l = 15 \text{ Hz}_{250 \text{ bps}}, b_l = 20 \text{ Hz}_{500 \text{ bps}}, \epsilon = 0.7$  环路的更新时间依据码速率的不同而不同。  $t_{s125 \text{ bps}} = 2 \text{ kHz}, t_{s250 \text{ bps}} = 4 \text{ kHz}, t_{s500 \text{ bps}} = 8 \text{ kHz}, K_a = P / (\frac{\pi}{2}), K_b = 2 \times \pi \times 64000 / 2^{32}$  ( $f_s = 64 \text{ kHz}, nco\_len = 32$ ) 由此可以依据公式 (5) (6) 推算出环路积分与直通支路的环路系数。位同步跟踪环路参数如下:  $b_l = 2 \text{ Hz}$  (三种码速率可以使用一个  $b_l$ ),  $\epsilon = 0.7, t_{s125 \text{ bps}} = 125 \text{ Hz}, t_{s250 \text{ bps}} = 250 \text{ Hz}, t_{s500 \text{ bps}} = 500 \text{ Hz}$ , 位同步环路系数的计算与副载波环路一致不再复述。

### 3 仿真实验与分析

根据以上算法的描述以及工程实现参数, 对三种码速率解调进行了仿真, 仿真条件是  $E_b/N_0$ : 16 dB, 多普勒: 2 Hz, 仿真时间 1 秒, 图 4 显示了三种码速率下同相支路与正交支路经过支路滤波器后输出的信号, 可以看出当副载波锁定后同相支路的积分值最大而正交支路的积分值最小, 图 5 是副载波和位同步跟踪环路 NCO 控制曲线, 从中可以看出三种码速率均实现了载波跟踪以及位同步, 实现正常的的数据解调。

算法仿真是建立在浮点运算基础上的, 最终采用 FPGA 实现时需要将上述运算定点化。FPGA 在实现下变频、自动增益控制、鉴相及积分清零等计算过程中均存在数据位宽的截断, 这无形中就会引入量化误差导致解调损失。在确定各个环路的数据位宽后采用定点仿真, 计算出在三种码速率下当输入  $E_b/N_0$  在  $0 \sim 20 \text{ dB}$  变化过程中, 解调器输出端的  $E_b/N_0$ , 并给出了误码率仿真曲线, 仿真结果表明, 该解调器在正常工作条件下 (应答机输入的  $E_b/N_0$  在  $16 \sim 20 \text{ dB}$ ) 的解调损失在  $2 \sim 2.5 \text{ dB}$  范围内, 均满足  $5 \times 10^{-6}$  的误码率要求。图 6 是算法定点化后的误码率仿真曲线。

### 4 可靠性设计

在多数卫星中, 遥控通道是地面上行控制卫星的唯一通道, 所以遥调解调的稳定性与可靠性尤其重要, 为此,

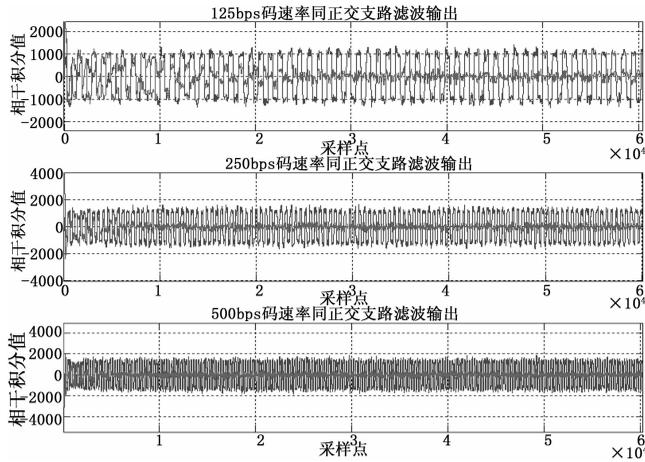


图 4 三种码速率下同相、正交支路滤波器的输出

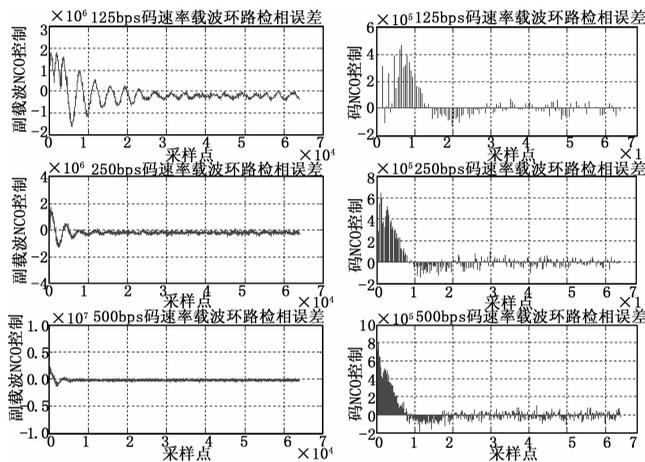


图 5 三种码速率下载波 NCO 及码 NCO 的误差控制曲线

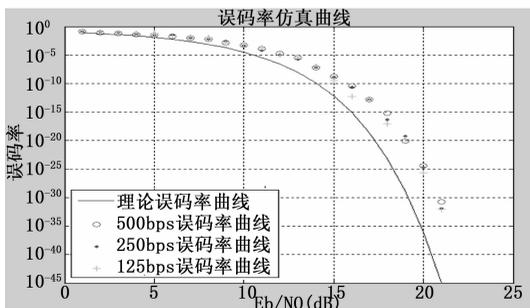


图 6 三种码速率定点解调误码率仿真曲线

需要增加对解调电路可靠性设计。遥控解调模块的副载波跟踪环路与码跟踪环路的环路滤波器均采用理想二阶环设计实现。由于遥控通道是采用突发通信工作模式，故大部分时间是没有副载波信号输入的，而是噪声。当输入的噪声不是理想白噪声时，环路滤波器中的积分支路，会逐渐偏离设计的中心值，长时间输入非白噪声信号会导致本地 NCO 的输出频率偏离中心频率 8 000 Hz 较远。

为了防止锁环的中心频率在无信号输入时偏离中心频率较远，以至在正常遥控信号到来时无法在引导序列内

实现副载波和位同步，可以采用如下两种方法。

#### 4.1 对环路滤波器输出频率进行限制的方法

仿真、分析副载波及码跟踪环路 NCO 控制字的震荡范围，合理控制频率区间对积分支路控制字输出幅度进行限制，以达到控制 NCO 最大输出频率的目的。将图 1 和图 3 中的环路滤波器改造如图 7 所示。该方法的缺点是如果频率范围限制小了会影响环路的自由震荡过程，导致锁定跟踪时间变长，如果限制过大同样会存在在引导序列内是否能实现副载波与码的同步问题。所以限制的幅度需要进行合理的仿真与设计。

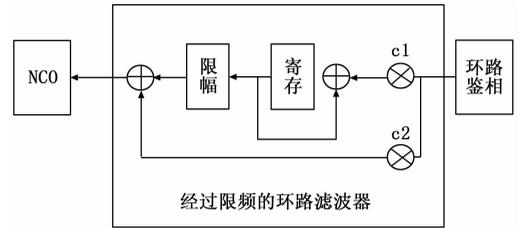


图 7 限频的环路滤波器

#### 4.2 采用副载波锁定检测的方法

采用副载波锁定检测的方法，实时监测副载波锁定状态，如果锁定则不对环路滤波器积分支路中的寄存器进行清零否则进行清零，保证锁相环路每次都是从中心频率开始跟踪输入信号。文献 [6-7] 提出了一种 M 进制调制信号的自归一化锁定检测算法，该算法描述如下：

$$y_{M,N} = \frac{1}{2N_k} \sum_{k=-N+1}^N \frac{\text{Re}[(I^2(k) + jQ^2(k))^M]}{(I^2(k) + jQ^2(k))^{M/2}} \quad (7)$$

其中：I(k)、Q(k) 表示滑动累加平均后，抽取前的同相与正交信号。针对遥控副载波调制，上述公式简化为：

$$y_{2,N} = \frac{1}{2N_k} \sum_{k=-N+1}^N \frac{I^2(k) - Q^2(k)}{I^2(k) + Q^2(k)} \quad (8)$$

确定采样点数 N，当  $y_{2,N} > \tau$  则认为锁定，否则失锁。在一定的 Eb/N0 的条件下，N 与  $\tau$  的选取关系确定了锁定检测的检测概率及虚警概率。

在 FPGA 实现时，选取采样点数为 N = 2 048，检测门限  $\tau = 0.5$ 。如果这 2048 个采样点中有 1024 个采样点都满足  $\tau > 0.5$  则认为是锁定，否则认为失锁。图 8 是在 125 bps 码速率条件下不同 Eb/N0 时通过 chipscope 软件采集 FPGA 内部数据的测试结果。图中的 counter 是采样点计数，large\_num 是满足阈值条件的采样点数，从中可以看出当 Eb/N0 > 10 dB 时，当 counte 为 2047 时 large\_num 已经显著大于 1024。

由于锁定检查开始时刻与地面发遥控上行是异步关系，在极端情况下当统计了 1024 点后收到地面发送的上行信号，导致检测到 2048 点时仍认为是失锁状态而给滤波器复位重新开始跟踪。为了避免上述情况发生，在系统应用时需要适当增加引导序列的长度来保证遥控信息的正常解调。

鉴于遥控通道对于整星安全性尤其关键，故尽量不要

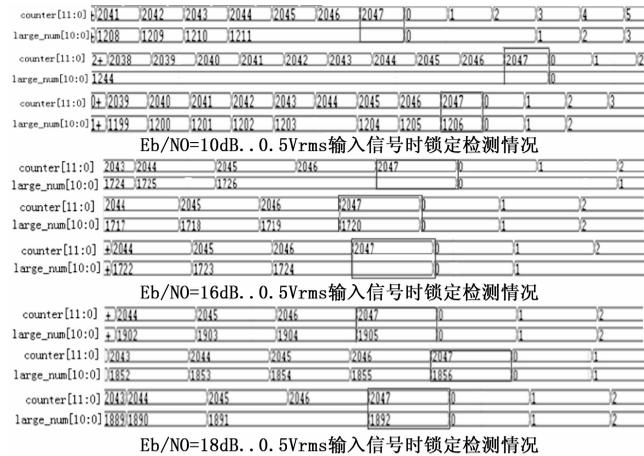


图 8 不同输入条件下阈值检测情况

使用 SEU 敏感的 SRAM 型号, 本项目选用 Actel 公司的反熔丝型 FPGA (AX500-1CQFP208), 最终实现资源占用情况见表 2 所示。

表 2 FPGA 资源使用统计

序号	逻辑资源	占用情况
1.	Combinational Cells	4783 of 5376(89%)
2.	Sequential Cells	2228 of 2688(83%)
3.	Total Cells	7011 of 8064(87%)

### 5 结论

本文介绍了一种适应多种码速率的遥控副载波数字化解调方法, 算法在 matlab 环境下进行了浮点与定点的仿真,

(上接第 182 页)

#### 参考文献:

[1] 田建伟, 刘 晶, 刘潇潇, 等. 用电信息采集终端远程升级平台设计与实现 [J]. 计算机应用与软件, 2014, 31 (1): 330-333.

[2] 戴 浩. 基于 FTP 的文件定时传输软件的设计与实现 [J]. 计算机应用与软件, 2013, 30 (1): 332-333.

[3] 徐旭光, 欧毓毅, 凌 捷, 等. 基于 PUF 的轻量级 RFID 安全认证协议 [J]. 计算机应用与软件, 2014, 31 (11): 302-306.

[4] 王 铮. 一种支持 OpenMP 线程绑定的分布式构件模型 [J]. 计算机应用与软件, 2013, 30 (3): 203-206.

[5] 金 杉, 李 秋. 基于多目标遗传算法的动态负载均衡方案 [J]. 计算机工程与科学, 2013, 35 (12): 102-106.

[6] 乔 付. 具有模糊多目标的网格任务调度算法 [J]. 计算机工程与科学, 2014, 36 (9): 1644-1649.

[7] 郝 秀, 宗 群, 李庆鑫, 等. 基于 dSPACE 的高超声速飞行器实时仿真平台 [J]. 计算机应用与软件, 2014, 31 (2): 52-54.

[8] 徐长彬. IEEE-1394b 光纤总线互连实时性分析 [J]. 科学技术与工程, 2012, 12 (21): 5347-5351.

最终采用反熔丝 FPGA 芯片设计实现。单机通过了与测控应答机联试, 各项测试表明, 解调算法及工程实现满足了误码率、频率跟踪误差及位同步时间等多项指标要求, 解调损失小, 可以作为遥控设备轻小型化和提高产品可靠性设计的一种技术手段。

#### 参考文献:

[1] 谢 钢. GPS 原理与接收机设计 [M]. 北京: 电子工业出版社, 2009.

[2] 姜 坤. 一种改进的数字 AGC 系统设计与仿真 [J]. 科技导报, 2011, 29 (33): 42-46.

[3] 张 欣. 扩频通信数字基带信号处理算法及其 VLSI 实现 [M]. 北京: 科学出版社, 2004.

[4] JAMES BAO-YEN TSUI GPS 软件接收机基础 (第二版) [M]. 北京: 电子工业出版社, 2007.

[5] 季仲梅. 通信中的同步技术及应用 [M]. 北京: 清华大学出版社, 2007.

[6] Yair Linn, A Self-Normalizing Symbol Synchronization Lock Detector for QPSK and BPSK [J]. IEEE Transactions on Wireless Communications, 2006, 5 (2).

[7] 郭黎利. 扩频通信系的 FPGA 设计 [M]. 北京: 国防工业出版社, 2013.

[8] 邓永铭. S 频段多模应答机的设计 [J]. 电讯技术, 2009, 49 (4).

[9] 司莹莹. 遥控副载波数字化解调技术研究 [J]. 电子器件, 2012, 35 (2): 181-183.

[10] 高翠东. 遥控副载波信号的软件解调方法 [J]. 信息安全与通信保密, 2009 (12): 50-52.

[9] 赵 彩, 丁 凰. 网络信息安全中 DES 数据加密技术研究 [J]. 计算机测量与控制, 2017, 25 (8): 241-243.

[10] Chen Shuzhen, Wang Zhu. The general term and property of the five order Fibonacci series [J]. Journal of Hainan Normal University ( Natural Science ), Hainan, 2014, 27: 241-244.

[11] Pohlig S, Hellman M. An Improved algorithm for computing Logarithm over GF (p) and its Cryptographic significance [J]. IEEE Transaction on Information Theory, Springer-Verlag, 1998, 1462, 458-471.

[12] Kocher P, Timing attacks on Implementations of Diffie-Hellman, RSA DSS and other systems [J]. Advances in Cryptology, 1996, 1109: 104-113.

[13] Jyotirmie P A, Ravi Kumar B, Chandra Sekhar A, Uma Devi S. A one to one Correspondence in elliptic curve cryptography [J]. International Journal of Mathematical archive, 2013, 4 (3): 300-304.

[14] Ravi Kumar B, Chandra Sekhar A, Appala Naidu G. A Diffie-Hellman key exchange for self-Encryption over points on the Elliptic Curve Cryptography [J]. Journal of Information and Computing Science, 2017, 12 (2): 83-87.